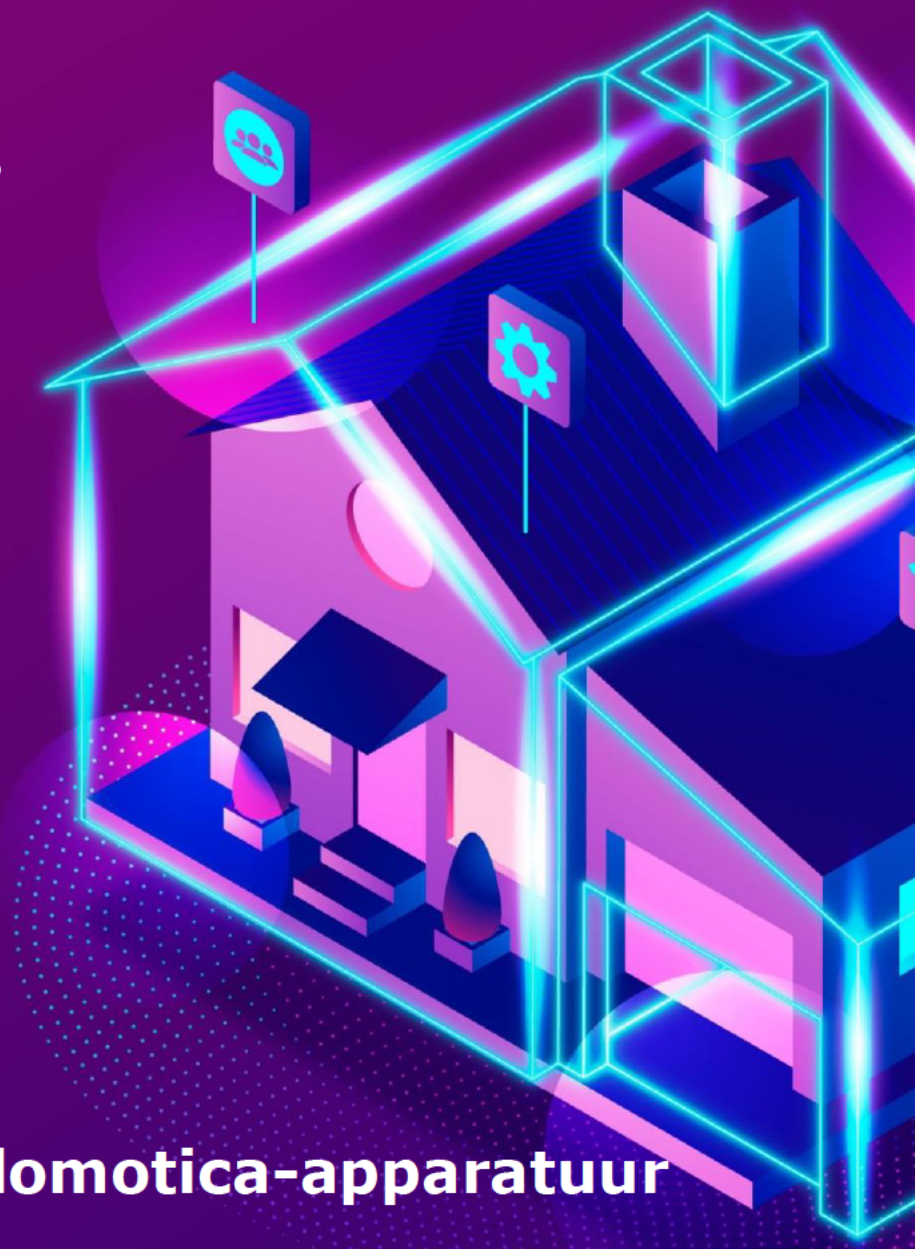
dialogic
innovatie • interactie

CREDS



Onderzoek domotica-apparatuur

In dit onderzoek analyseren we voor 15 domotica-apparaten uit verschillende productgroepen hoe deze zich verhouden tot regelgeving op het gebied van functionaliteit, compatibiliteit en interoperabiliteit, het updatebeleid en de digitale veiligheid. We kijken naar de informatie die verkoper en fabrikant voor en tijdens de aankoop verstrekken en vergelijken deze met de feitelijke eigenschappen van de apparaten. We beproeven daarnaast de digitale veiligheid. We volgen de apparaten gedurende drie maanden om te kijken of er updates worden aangeboden, en of er zich daardoor wezenlijke veranderingen voordoen in de eigenschappen op gebied van functionaliteit, compatibiliteit en interoperabiliteit. Naast een nulmeting biedt dit onderzoek toezichthouders kennis en inzichten die relevant kunnen zijn voor het vormgeven van toezicht.

Ir. Tommy van der Vorst, mr. drs. Melvin Hanswijk,
Pim Verhagen MSc & Ralf Bardoel

Opdrachtgever:	**Publicatienummer:**	**Datum:**
Autoriteit Consument & Markt en Agentschap Telecom	2021.198.2223 Versie 1.3.1105	Utrecht, 31 augustus 2022

Inhoudsopgave

Citeren als: Dialogic, van der Vorst, T., Hanswijk, M., Verhagen, P. & Bardoel, R. (2022). *Onderzoek domotica-apparatuur*. In opdracht van de Autoriteit Consument & Markt en het Agentschap Telecom, Den Haag.

Met medewerking van Carolien Spoelder, Wazir Sahebali, Nino van Sambeek en Floris Donath (Dialogic).

Met medewerking van prof. dr. Marco Loos (Universiteit van Amsterdam) – juridisch kader en juridische duiding bij de resultaten.

Het CREDS-testteam bestond uit Ralf Bardoel, Ilke Tosunoglu, Jose Exposito, Robert van Hees en Daan Wagenaar.

Managementsamenvatting

In dit onderzoek staat centraal in welke mate domotica-apparaten die op de Nederlandse markt worden aangeboden voldoen aan wet- en regelgeving op het gebied van de digitale veiligheid van de apparaatsoftware (onderzoeksvraag 1) en informatieverstrekking over compatibiliteit, functionaliteit, interoperabiliteit, en het updatebeleid (onderzoeksvraag 2). De regelgeving betreft de Europese Richtlijn voor levering van digitale inhoud (EU 2019/770), de Richtlijn verkoop goederen (2019/771), de Moderniseringsrichtlijn (2019/2161) en de Radiorichtlijn (2014/53), inclusief gedelegeerde handeling. Naast een nulmeting biedt dit onderzoek toezichthouders kennis en inzichten die relevant kunnen zijn voor het vormgeven van toezicht op basis van de bovengenoemde regelgeving.

We onderzoeken een steekproef van 15 domotica-apparaten uit vijf verschillende productgroepen en analyseren of deze voldoen aan de regelgeving. We kijken naar de informatie die de verkoper en fabrikant voor, tijdens en na de aankoop verstrekken, en vergelijken deze met de feitelijke eigenschappen van de apparaten. We nemen de apparaten in gebruik en volgen ze gedurende drie maanden. Hierbij meten we of er updates worden aangeboden en of er zich wezenlijke veranderingen voordoen in de eigenschappen op gebied van functionaliteit, compatibiliteit en interoperabiliteit. Daarnaast meten we de digitale veiligheid op basis van analyseraamwerken en diepgaande (risico-gestuurde) analyse.

De hieronder samengevatte bevindingen zijn geformuleerd door de onderzoekers op basis van de steekproefresultaten, en tot stand gekomen binnen de afbakening en beperkingen van het onderzoek. De specifieke bevindingen per apparaat in de steekproef zijn te vinden in Bijlage 3. De bevindingen dienen niet te worden geïnterpreteerd als zienswijze of standpunt van het AT noch de ACM.

Onderzoeksvraag 1. Hoe veilig is de software van domotica-apparaten op de Nederlandse markt?

Het basisniveau van digitale veiligheid van de software op de onderzochte domotica-apparaten is te typeren als voldoende, maar niet perfect:

- Eén domotica-apparaat in de steekproef bevatte een misbruikbare beveiligings-zwakheid. Bij de andere 14 apparaten zijn geen (met directe netwerktoegang tot het apparaat) misbruikbare beveiligingszwakheden gevonden.
- Acht apparaten in de steekproef voldoen ieder niet aan ten minste één vereiste uit de gehanteerde analyseraamwerken. De gebreken betreffen het niet volgen van 'security best practices', waaronder met name de wijze van gebruik van TLS voor beveiliging van verbindingen en het prijsgeven van software- en versie-informatie.
- Domotica-apparaten maken in plaats van rechtstreekse communicatie over het lokale thuisnetwerk steeds vaker gebruik van een onlinedienst van de fabrikant. Hoewel dit de veiligheid van de apparaten ten opzichte van een aanvaller met netwerktoegang tot het apparaat kan verhogen, is de veiligheid wel sterk(er) afhankelijk van de veiligheid van de onlinedienst.
- Domotica-apparaten zijn voor ingebruikname vaak voorzien van relatief oude software. Niet alle apparaten dwingen af dat de meest recente versie wordt geïnstalleerd bij ingebruikname. Gebruikers kunnen daarom zonder het te weten gebruik maken van een verouderde, kwetsbare softwareversie.

Updates

- In de steekproef ontvingen zeven van de 15 apparaten gedurende de gebruiksperiode geen enkele update (buiten een eventuele update direct na ingebruikname). Dit terwijl uit de analyse van digitale veiligheid verbeterpunten blijken die met een update zouden kunnen worden verholpen.
- Wanneer een apparaat wordt gebruikt in combinatie met een interoperabel apparaat van een andere fabrikant (zoals een domotica-basisstation) dan is niet gegarandeerd dat het apparaat (automatisch of handmatig) kan worden geüpdatet. Gebruikers kunnen daarom zonder het te weten gebruik maken van een verouderde, kwetsbare softwareversie.

Onderzoeksvraag 2. Welke informatie verstrekken de verkopers en de producenten van domotica-apparaten op de Nederlandse markt, en strookt dit met de daadwerkelijke kenmerken van het apparaat, en het daarna uitgevoerde updatebeleid?

Functionaliteit, compatibiliteit en interoperabiliteit

De door de verkopers en fabrikanten (precontractueel) verstrekte informatie over de functionaliteit, compatibiliteit en interoperabiliteit is summier:

- Voor ieder online aangeschaft domotica-apparaat in de steekproef ontbrak ten minste één door ons onderzocht kenmerk ten aanzien van de functionaliteit, compatibiliteit en interoperabiliteit in de door de verkoper (precontractueel, maar ook tijdens ingebruikname en de gebruiksperiode) verstrekte informatie. Dit geldt ook voor de informatie verstrekt door de fabrikant op moment van aankoop. Soms *verschilt* de informatie die de verkoper verstrekt van de informatie van de fabrikant.
- Bij aankopen in een fysieke winkel is de informatieverstrekking veel minder volledig, minder exact en gevarieerder dan bij online aankopen, zelfs wanneer expliciet wordt gevraagd naar bijvoorbeeld de minimale updatetermijn.
- De meeste domotica-apparaten in de steekproef zijn afhankelijk van een onlinedienst van de fabrikant voor het realiseren van slimme functionaliteit. Bij de meerderheid van de onderzochte apparaten is het voor de consument (precontractueel noch daarna) niet inzichtelijk tot wanneer de fabrikant deze dienst minimaal blijft aanbieden.

De online aangeschafte domotica-apparaten in de steekproef voldoen gedurende de onderzoeksperiode (op hoofdlijnen en voor zover wij konden beoordelen) wel aan wat in de verstrekte precontractuele informatie is beschreven over functionaliteit, compatibiliteit en interoperabiliteit.

Updatebeleid

De door de verkopers en fabrikanten (precontractueel) verstrekte informatie over het updatebeleid is summier:

- Voor zes van de tien online aangeschafte apparaten is door de verkoper precontractueel geen informatie verstrekt over het updatebeleid. Bij vier online aankopen gaf de verkoper wel een termijn voor ondersteuning aan. Wanneer er (door de verkoper of de fabrikant) een minimumtermijn voor updates wordt verstrekt, is deze vaak relatief geformuleerd ("N jaar ondersteuning").
- Voor slechts twee domotica-apparaten (van de acht online aangeschafte waarvoor dit van toepassing was) verstrekte de verkoper informatie over de specifieke (minimum)versienummers van besturingssystemen waarop de bijbehorende apps werken, terwijl deze ondersteuning gedurende de gebruikersperiode wel kan veranderen.

- Een aantal apparaten kon pas worden bijgewerkt na acceptatie van voorwaarden.

Aanbevelingen ten aanzien van de werkwijze

- We adviseren om onderzoeken naar het updatebeleid van domotica-apparaten over een langere periode (bijvoorbeeld één of twee jaar) uit te voeren. Met een meting over langere tijd kunnen met hogere zekerheid uitspraken worden gedaan over de consistentie van het updaten na het bekend worden van beveiligingszwakheden.
- We adviseren om bij de beoordeling van de digitale veiligheid van domotica-apparaten (ook) gebruik te maken van een raamwerk dat past bij de (hedendaags dominante) architectuur waarin een clouddienst van de fabrikant centraal staat. Er kan hierbij worden gewerkt met certificeringen. De dienst kan daarnaast van buitenaf getest worden (mits hiervoor vrijwaringsverklaringen zijn verkregen).
- We adviseren nadere analyse van de voorwaarden die door gebruikers moeten worden geaccepteerd om slimme functies van het product (waaronder de updatefunctie) te kunnen gebruiken.

1 Inleiding

1.1 Achtergrond

Het Agentschap Telecom (hierna: AT) en de Autoriteit Consument & Markt (ACM) hebben Dialogic gevraagd onderzoek uit te voeren naar hoe het huidige aanbod van domotica-apparaten op de Nederlandse markt zich verhoudt met een aantal vereisten op grond van (primair) de volgende regelgeving:

- **Richtlijn levering digitale inhoud**: Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten.

- **Richtlijn verkoop goederen**: Richtlijn (EU) 2019/771 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de verkoop van goederen, tot wijziging van Verordening (EU) 2017/2394 en Richtlijn 2009/22/EG, en tot intrekking van Richtlijn 1999/44/EG.

- **Moderniseringsrichtlijn**: Richtlijn (EU) 2019/2161 van het Europees Parlement en de Raad van 27 november 2019 tot wijziging van Richtlijn 93/13/EEG van de Raad en Richtlijnen 98/6/EG, 2005/29/EG en 2011/83/EU van het Europees Parlement en de Raad wat betreft betere handhaving en modernisering van de regels voor consumentenbescherming in de Unie, waaronder de Richtlijn oneerlijke handelspraktijken (2005/29/EG betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt).

- **Radiorichtlijn**: Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 over de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG als aangevuld bij Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 Juli 2018. De gedelegeerde verordening 2022/30 past deze richtlijn aan, waardoor vanaf 1 augustus 2024 cyberveiligheidseisen worden gesteld aan radioapparaten. [1]

Domotica betreft het automatiseren van processen in en om het huis en soortgelijke omgevingen, een en ander in de breedste zin van het woord. Domotica-apparatuur bestaat veelal uit een of meerdere sensoren die informatie uit de omgeving verzamelen, logica (in hard- en software) die deze gegevens interpreteert, en actuatoren die de omgeving (op basis van sensorgegevens en soms ook door de software autonoom gemaakte beslissingen) kunnen beïnvloeden.

1.2 Doel van het onderzoek

Dit onderzoek heeft als doel te meten hoe domotica-apparaten op de Nederlandse markt zich verhouden tot de hierboven genoemde regelgeving. De onderzoeksvragen luiden als volgt:

1. Hoe veilig is de software van domotica-apparaten (hierna 'apparaatsoftware') op de Nederlandse markt?

2. Welke informatie verstrekken de verkopers en de producenten van domotica-apparaten op de Nederlandse markt, en strookt dit met de daadwerkelijke kenmerken van het apparaat, en het daarna uitgevoerde updatebeleid?

In dit onderzoek onderscheiden we ter beantwoording van de onderzoeksvragen de volgende aspecten: (1) de functionaliteit, (2) de compatibiliteit en interoperabiliteit, (3) het updatebeleid en (4) de digitale veiligheid van het apparaat.

We beantwoorden de onderzoeksvragen voor een (representatieve en navolgbare) steekproef van 15 domotica-apparaten verdeeld over vijf productcategorieën, die op de Nederlandse markt worden aangeboden. Naast de individuele resultaten per apparaat beschrijven we in dit onderzoek ook het algemene beeld op basis van de steekproef.

Een tweede doel van dit onderzoek is om inzicht krijgen in de werkwijze, de opgedane kennis en de praktijkervaringen bij het uitvoeren van de bovengenoemde meting. Deze inzichten kunnen de toezichthouders helpen bij het vormgeven van handhaving.

Het is van belang dat de beoordelingen navolgbaar zijn voor het AT en de ACM – in dit rapport besteden we dan ook uitgebreid aandacht aan het beschrijven van de gevolgde procedure.

We benadrukken dat de in dit onderzoek gehanteerde methoden, afbakeningen, criteria en dergelijke weliswaar zijn overlegd met het AT en de ACM, maar uiteindelijk de keuze zijn geweest van het onderzoeksteam. Zienswijzen en standpunten in dit rapport komen niet noodzakelijkerwijs overeen met die van het AT noch de ACM.

De juridische duidingen in hoofdstuk 2 (juridisch kader), hoofdstuk 4 (resultaten) en elders in het rapport zijn die van de onderzoekers en niet van het AT noch de ACM.

1.3 Leeswijzer

Allereerst schetsen we in hoofdstuk 2 het analysekader dat van toepassing is op dit onderzoek. Daarbij gaan we primair in op de juridische aspecten. In hoofdstuk 3 komen we mede op basis van het analytisch kader tot een methodiek voor het onderzoeken van domotica-apparaten. In hoofdstuk 4 beschrijven we de resultaten van het uitvoeren van deze methodiek voor een steekproef van 15 apparaten. De gedetailleerde resultaten per apparaat zijn opgenomen als bijlage. In hoofdstuk 5 geven we onze conclusies en aanbevelingen op basis van de resultaten van de steekproef.

2 Analysekader

In dit hoofdstuk bespreken we de relevante juridische kaders ten aanzien van de onderzoeksvraag. Met deze kaders kan worden bepaald aan welke vereisten domotica-apparaten die op de Nederlandse markt worden aangeboden zich zouden moeten houden. We bekijken de juridische kaders vanuit twee perspectieven: het consumentenrecht (primair het werkveld van de ACM) en de Radiorichtlijn (primair het werkveld van het AT).

2.1 Juridisch kader: consumentenrecht

Met de inwerkingtreding van de Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud en de Implementatiewet richtlijn modernisering consumentenbescherming zijn de regeling over informatieplichten en bedenktijden (Afd. 6.5.2B BW[1]) en de regeling van de consumentenkoop (Titel 7.1) ingrijpend gewijzigd, en is een nieuwe Titel 7.1AA BW betreffende overeenkomsten voor de levering van digitale inhoud en digitale diensten tussen handelaren en consumenten van kracht geworden. Deze regelingen bevatten samen de belangrijkste regels die gelden voor de levering van domotica-apparaten. Deze wetten zijn in de laatste fase van dit onderzoek in werking getreden.[2]

Domotica-apparaten moeten juridisch worden gekwalificeerd als zaken met digitale elementen (art. 7:5 lid 1 onder b BW).[3] Het gaat immers steeds om een roerende zaak waarin digitale inhoud[4] of een digitale dienst[5] is verwerkt of die daarmee onderling verbonden is, op zodanige wijze dat het ontbreken daarvan ertoe zou leiden dat de roerende zaak zijn functies niet kan vervullen.

2.1.1 Precontractuele informatieplichten (inleiding)

De precontractuele informatieplichten zijn neergelegd in de artikelen 6:230l en art. 6:230m BW. Deze informatieplichten brengen mee dat over verschillende onderwerpen informatie moet worden verstrekt, en wel op zodanige wijze dat de 'gemiddelde consument' – die gemiddeld geïnformeerd, omzichtig en oplettend is[6] – na lezing van de informatie een geïnformeerde beslissing kan nemen over de aanschaf van het domotica-apparaat. Van 'de gemiddelde consument' mag wel worden verwacht dat hij de verstrekte informatie

---

[1] Burgerlijk Wetboek

[2] *Stb.* 2022, 157; *Stb.* 2022, 164.

[3] Een *'zaak met digitale elementen*' wordt in art. 7:5 lid 1 onder b BW omschreven als 'een roerende zaak waarin digitale inhoud of een digitale dienst is verwerkt of die daarmee onderling verbonden is, op zodanige wijze dat het ontbreken daarvan ertoe zou leiden dat de zaak zijn functies niet kan vervullen'. Dezelfde definitie is opgenomen in art. 6:230g lid 1 onder r BW.

[4] Het begrip '*digitale inhoud'* wordt in art. 6:230g lid 1 onder i, art. 7:5 lid 1 onder c en art. 7:50aa onder a BW steeds omschreven als 'gegevens die in digitale vorm worden geproduceerd en geleverd'.

[5] Het begrip '*digitale dienst'* wordt in art. 6:230g lid 1 onder t, art. 7:5 lid 1 onder d en art. 7:50aa onder b BW omschreven als 'i) een dienst die de koper in staat stelt gegevens in digitale vorm te creëren, te verwerken of op te slaan, of toegang tot die gegevens te krijgen, of ii) een dienst die voorziet in de mogelijkheid tot het delen van gegevens of andere interactie met gegevens in digitale vorm die door de koper of door andere gebruikers van die dienst worden geüpload of gecreëerd'.

[6] Vgl. HvJ EG 16 juli 1998, nr. C-210/96, ECLI:EU:C:1998:369 (Gut Springenheide GmbH/Oberkreisdirektor des Kreises Steinfurt).

doorleest, maar niet dat hij zelf op zoek gaat naar informatie die hem verstrekt had moeten worden. Het enkele feit dat informatie op de website van de handelaar beschikbaar was of de consument deze had kunnen raadplegen door te klikken op links, is niet voldoende om aan de informatieplicht te voldoen.[7] Het Hof van Justitie heeft inmiddels duidelijk gemaakt dat het in beginsel is toegestaan dat de informatie in algemene voorwaarden of in andere bijgevoegde documenten wordt opgenomen.[8] Dat laat echter onverlet dat de informatie 'op duidelijke en begrijpelijke wijze'[9] moet zijn verstrekt. Wanneer daarvan sprake is moet zich verder uitkristalliseren. Aan dit transparantievereiste lijkt echter niet te zijn voldaan als de consument de informatie moet zoeken omdat de informatie *op een misleidende of versluierde wijze* is verstrekt, bijvoorbeeld door deze in een artikel in de algemene voorwaarden op te nemen dat ogenschijnlijk over een ander onderwerp gaat. Zo zal informatie over de voornaamste kenmerken van de zaak wel mogen worden opgenomen in een artikel over 'het product', 'producteigenschappen' of 'het gebruik van het product', maar niet in een artikel dat gaat over 'geschillen'. Ook mag van de consument niet worden verwacht dat hij een aantal maal doorklikt om de juiste informatie te vinden. Om te voldoen aan het transparantievereiste moet de te verstrekken informatie derhalve op eenvoudige wijze kunnen worden geraadpleegd en gelezen.

Op grond van het (aan de Moderniseringsrichtlijn[10] aangepaste) art. 6:230l BW dient de verkoper van domotica-apparaten die binnen een verkoopruimte (zoals een winkel)[11] worden aangeschaft, de consument-koper vóór of bij contractsluiting op duidelijke en begrijpelijke wijze te informeren over de belangrijkste kenmerken van het apparaat (sub a), voor zover deze informatie niet al uit de context duidelijk is. Voor zover de overeenkomst op afstand (zoals via een webwinkel of een online platform)[12] of buiten een verkoopruimte (zoals bij een verkoopdemonstratie of aan de deur bij de consument thuis)[13] wordt gesloten, dient deze informatie steeds te worden verstrekt (art. 6:230m lid 1 sub a BW).

---

[7] Vgl. in dit verband reeds Hof van Justitie 5 juli 2012, zaak C-49/11, ECLI:EU:C:2012:419, *NJ* 2012/542 m.nt. M.R. Mok, *TvC* 2013/123 m.nt. S. De Pourcq (Content Services Ltd)

[8] Hof van Justitie 24 februari 2022, zaak C-536/20, ECLI:EU:C:2022:112 (Tiketa).

[9] Zie de aanhef van art. 6:230l en art. 6:230m lid 1 BW.

[10] Richtlijn 2019/2161, *PubEU* 2019, L 328/7.

[11] Het begrip 'verkoopruimte' omvat volgens de definitie in art. 6:230g lid 1 onder g BW 'iedere onverplaatsbare ruimte voor detailhandel waar de handelaar op permanente basis zijn activiteiten uitoefent', en 'iedere verplaatsbare ruimte voor detailhandel waar de handelaar gewoonlijk zijn activiteiten uitoefent'.

[12] Een 'overeenkomst op afstand' is een 'overeenkomst die tussen de handelaar en de consument wordt gesloten in het kader van een georganiseerd systeem voor verkoop of dienstverlening op afstand zonder gelijktijdige persoonlijke aanwezigheid van handelaar en consument en waarbij, tot en met het moment van het sluiten van de overeenkomst, uitsluitend gebruik wordt gemaakt van een of meer middelen voor communicatie op afstand' art. 6:230g lid 1 onder e BW.

[13] Een 'overeenkomst buiten verkoopruimte' omvat volgens art. 6:230g lid 1 onder f BW iedere overeenkomst tussen de handelaar en de consument, die wordt gesloten in gelijktijdige persoonlijke aanwezigheid van de handelaar en de consument (1^0) op een andere plaats dan de verkoopruimte van de handelaar of waarvoor door de consument een aanbod is gedaan onder dezelfde omstandigheden, (2^0) in de verkoopruimte van de handelaar of met behulp van een middel voor communicatie op afstand, onmiddellijk nadat de consument persoonlijk en individueel is aangesproken op een plaats die niet de verkoopruimte van de handelaar is, in gelijktijdige persoonlijke aanwezigheid van de handelaar en de consument; of (3°) tijdens een excursie die door de handelaar is georganiseerd met als doel of effect de promotie en de verkoop van zaken of diensten aan de consument.

Voor de invulling van wat onder de 'voornaamste kenmerken' van de zaak moet worden begrepen, kan aansluiting worden gezocht bij de in art. 7:18 lid 2 BW genoemde objectieve conformiteitsvereisten. Op grond van deze bepaling moet de zaak immers, voor zover relevant, (a) geschikt zijn voor de doeleinden waarvoor zaken van hetzelfde type gewoonlijk worden gebruikt, (b) beschikken over de kwaliteit van en beantwoorden aan de beschrijving van een monster of model, dat de verkoper aan de koper voor het sluiten van de overeenkomst ter beschikking heeft gesteld, (c) worden geleverd met de toebehoren, waaronder verpakking, installatie-instructies of andere instructies, die de koper redelijkerwijs mag verwachten, en (d) de hoeveelheid hebben en de kenmerken bezitten, onder meer met betrekking tot duurzaamheid, functionaliteit, compatibiliteit en beveiliging, die voor hetzelfde type zaken normaal zijn en die de koper redelijkerwijs mag verwachten gelet op de aard van de zaak. Aannemelijk lijkt dat de onder (a), (b) en (d) genoemde kenmerken als de 'voornaamste kenmerken in de zin van art. 6:230l onder a en art. 6:230m lid 1 onder a BW moeten worden gezien.

Daarnaast moet de consument volgens de Europese Commissie worden geïnformeerd over alle productkenmerken en beperkende voorwaarden die *afwijken* van wat de gemiddelde consument normaliter van de betrokken categorie of soort goederen of diensten verwacht. De Commissie merkt in dit verband op dat dergelijke afwijkingen waarschijnlijk van invloed zullen zijn op het besluit van de consument of hij de overeenkomst wil sluiten, en zo ja: onder welke voorwaarden. [2, p. 27] Voor zover de consument in verband met de sluiting of nakoming van de overeenkomst persoonsgegevens[14] aan de handelaar verstrekt, moet de handelaar de consument bovendien informeren over de doeleinden van de verwerking op het moment dat de persoonsgegevens worden verkregen. [2, p. 27]

Deze informatie moet steeds worden verstrekt indien de overeenkomst op afstand of buiten verkoopruimte is gesloten, en slechts indien deze informatie niet al uit de context duidelijk is indien de overeenkomst binnen een verkoopruimte is gesloten. Wanneer dergelijke informatie niet wordt verstrekt, levert dat een misleidende omissie op (art. 6:193d lid 1 en 2 BW). Dat geldt ook als de informatie weliswaar wel wordt verstrekt, maar op zodanige wijze verborgen wordt gehouden of de informatie op onduidelijke, onbegrijpelijke of dubbelzinnige wijze is verstrekt dat de gemiddelde consument deze informatie niet zou betrekken in zijn beslissing om de overeenkomst te sluiten (art. 6:193d lid 3 jo. 193f onder b BW).

Wanneer de informatie over de voornaamste kenmerken van het domotica-apparaat niet is verstrekt, kan de consument die het product heeft gekocht mogelijk een andere beslissing hebben genomen over de aanschaf van het domotica-apparaat dan hij zou hebben genomen indien de informatie wel (op duidelijke en begrijpelijke wijze) zou zijn verstrekt. De consument kan in een dergelijk geval de overeenkomst vernietigen (art. 6:193j lid 3 BW). Bovendien geldt volgens de Hoge Raad ten aanzien van de informatieplicht voor overeenkomsten die op afstand of buiten een verkoopruimte zijn gesloten, dat de rechter gehouden is ambtshalve te toetsen of zij is nagekomen, en dient hij zo nodig op de voet van art. 3:40 lid 2 BW ambtshalve over te gaan tot algehele of gedeeltelijke vernietiging van de overeenkomst (tenzij, uiteraard, de consument zich daartegen zou verzetten).[15] Of deze uitspraak ook geldt ten aanzien van overeenkomsten die in een verkoopruimte gesloten zijn, is onduidelijk; de Hoge Raad heeft zich daarover tot op heden nog niet uitgelaten.

---

[14] Als bedoeld in art. 4, onderdeel 1, van de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679, *Pub. EU* 2016 L 119), zie art. 6:230g lid 1 onder s BW.

[15] Zie HR 12 november 2021, ECLI:NL:HR:2021:1677, *NJ* 2022/89 m.nt. C.M.D.S. Pavillon.

2.1.2 Specifieke informatieplichten t.a.v. functionaliteit, compatibiliteit en interoperabiliteit

Het begrip 'functionaliteit' wordt in art. 6:230g lid 1 onder x BW gedefinieerd als 'het vermogen van de digitale inhoud of digitale dienst om zijn functies te vervullen met betrekking tot het doel ervan'. In de parlementaire geschiedenis wordt op dit punt opgemerkt dat het begrip verwijst naar de manieren waarop digitale inhoud of een digitale dienst kan worden gebruikt. In dit verband wordt opgemerkt dat technische beperkingen gevolgen kunnen hebben voor de mate waarin de digitale inhoud of digitale dienst alle beoogde functies kan vervullen. Zo kan regiocodering het onmogelijk maken voor de consument om op de plaats waar hij verblijft een bepaald film- of audiobestand af te spelen of streamingdiensten af te nemen.[16] Een andere technische beperking is het beperken van de mogelijkheid tot het maken van kopieën. Technische beperkingen kunnen ook specifieke functies van het apparaat uitschakelen of alleen tegen bijbetaling beschikbaar maken. Informatie over de functionaliteit van de zaak met digitale elementen en eventuele technische beperkingen dient op zodanige wijze aan de consument te worden medegedeeld dat de 'gemiddelde consument' deze beperkingen begrijpt en mede op basis daarvan zijn beslissing neemt over de aanschaf van het apparaat.

Uit het voorgaande blijkt dat het begrip functionaliteit in het kader van de informatieplichten van art. 6:230l onder g en 230m lid 1 onder r BW dus alleen betrekking op de mogelijkheid *van de digitale inhoud of dienst* om zijn functies te vervullen.[17] Dat is in afwijking van de betekenis van dit begrip in het kader van de conformiteit, waar in par. 1.1.3 op zal worden ingegaan.

Iets soortgelijks geldt ten aanzien van de begrippen 'compatibiliteit' en 'interoperabiliteit', waar de informatieplichten van art. 6:230l onder h en art. 6:230m lid 1 onder s BW betrekking op hebben. Met 'compatibiliteit' is volgens art. 6:230g lid 1 onder w bedoeld *'het vermogen van de digitale inhoud of digitale dienst om te functioneren met hardware of software waarmee digitale inhoud of digitale diensten van hetzelfde type gewoonlijk worden gebruikt, zonder dat die digitale inhoud of digitale dienst moeten worden omgezet'*.[18] De informatieplichten van art. 6:230l onder h en art. 6:230m lid 1 onder s BW zijn erop gericht om de consument voor contractsluiting in staat te stellen te beoordelen of de zaak met digitale elementen aansluit bij de digitale omgeving waarbinnen de zaak met digitale elementen zal moeten functioneren. Het gaat daarbij bijvoorbeeld om het besturingssysteem van de software en om kenmerken van de hardware. In de parlementaire geschiedenis wordt hierbij het voorbeeld gegeven dat de grafische kaart van zijn computer moet voldoen om een bepaald computerspel te spelen.[19] Dat betekent dat de verkoper de consument moet informeren over de belangrijkste technische kenmerken van het domotica-apparaat en de technische vereisten waaraan voldaan moet zijn om het domotica-apparaat te kunnen laten functioneren binnen de digitale omgeving van de consument. Daartoe zal de verkoper in ieder geval informatie moeten verstrekken over de minimaal vereiste systeemversie van de besturingssoftware en de versie van de software die het domotica-apparaat zelf gebruikt. Ook wanneer de digitale inhoud slechts

---

[16] *Kamerstukken II* 2021/22, 35 940, nr. 3, p. 35, onder verwijzing naar overweging 36 in de preambule bij de Moderniseringsrichtlijn.

[17] Vgl in deze zin ook art. 7:50aa onder j BW.

[18] Art. 7:50aa onder i BW bevat een hiermee overeenkomende definitie.

[19] *Kamerstukken II* 2021/22, 35 940, nr. 3, p. 35.

ondersteund wordt door *verouderde* besturingssoftware, is dat informatie die door de verkoper aan de consument moet worden gemeld.

Met 'interoperabiliteit' wordt volgens art. 6:230g lid 1 onder y BW gedoeld op '*het vermogen van de digitale inhoud of digitale dienst om te functioneren met hardware of software die verschilt van die waarmee digitale inhoud of digitale diensten van hetzelfde type gewoonlijk worden gebruikt.*'[20] Bij interoperabiliteit kan worden gedacht aan de mogelijkheid om informatie uit te wisselen met andere software en hardware en om vervolgens die informatie ook te kunnen gebruiken.[21] Bij interoperabiliteit kan worden gedacht aan de mogelijkheid om informatie uit te wisselen met andere software en hardware en om vervolgens die informatie ook te kunnen gebruiken.[22] Het in dit verband in de parlementaire geschiedenis gegeven voorbeeld is misschien wat minder gelukkig: volgens de memorie van toelichting is sprake van interoperabiliteit als een app kan worden gebruikt op smartphones met verschillende besturingssystemen.[23] Die situatie lijkt echter (naar geldend recht) het geval van *compabiliteit* te betreffen: het betreft de vraag of de app zonder dat omzetting nodig is, gebruikt kan worden op een smartphone met een bepaald besturingssysteem. Van interoperabiliteit is sprake als de consument de app van het ene apparaat op een ander apparaat kan zetten, met andere woorden: of de app kan worden overgezet van de ene telefoon op de andere telefoon. Daarvoor is in ieder geval vereist dat de beide smartphones compatibel zijn met de app, maar geldt bovendien de eis van 'overzetbaarheid', bijvoorbeeld door middel van speciale software. De op dit punt in het kader van art. 6:230l onder h en art. 6:230m lid 1 onder s BW te verstrekken informatie is erop gericht om de consument voor contractsluiting in staat te stellen te beoordelen of de zaak met digitale elementen aansluit bij de verdere digitale omgeving van de consument. Deze informatie moet onder meer duidelijk maken in hoeverre de consument '*locked in'* een bepaalde digitale omgeving is doordat de digitale inhoud alleen kan worden overgezet naar andere dragers van dezelfde producent of dat de digitale inhoud juist eenvoudig kan worden overgezet op andere dragers die door andere producenten zijn geproduceerd maar die gebruik maken van dezelfde besturingssoftware.

Tot de inwerkingtreding van de Implementatiewet richtlijn modernisering consumentenbescherming bevatten art. 6:230l onder g en h en art. 6:230m lid 1 onder r en s BW de verplichting van de handelaar om consumenten te informeren over de functionaliteit en interoperabiliteit van *digitale inhoud*. Onder het begrip 'interoperabiliteit' moest destijds tevens worden verstaan de compabiliteit daarvan. In de door de Europese Commissie in 2014 gepubliceerde Leidraad voor de uitleg van de richtlijn [3][24] werd duidelijk gemaakt dat ten aanzien van digitale inhoud *'de beschrijving van de voornaamste kenmerken van het digitale product ook informatie [moet] bevatten over zijn functionaliteit en interoperabiliteit'*, aangezien een consument zonder dergelijke informatie niet kan beoordelen of het product voldoet aan zijn eisen. [3, p. 78] De Commissie gaf daarbij onder meer als voorbeeld dat informatie over het bestandstype nuttig kan zijn voor een consument die wil beoordelen of een downloadbare song kan worden opgenomen in zijn huidige muziekcollectie van bijvoorbeeld niet-gecomprimeerde mediabestanden. Voor gestreamde muziek kan het bestandstype minder relevant zijn, zo stelde de Commissie. [3, p. 78] De Leidraad 2014 maakt duidelijk dat de informatieplicht over de functionaliteit

---

[20] Vgl. ook het hiermee overeenstemmende art. 7:50aa onder k BW.

[21] Zie overweging 36 in de preambule van de Moderniseringsrichtlijn.

[22] Zie overweging 36 in de preambule van de Moderniseringsrichtlijn.

[23] *Kamerstukken II* 2021/22, 35 940, nr. 3, p. 35.

[24] De Leidraad 2014 is inmiddels vervangen door de eerder genoemde Richtsnoeren 2021.

en interoperabiliteit van de digitale inhoud te zien is als een nadere toespitsing van de informatie over de 'voornaamste kenmerken van de zaken of diensten' als bedoeld in art. 6:230l onder a en art. 6:230m lid 1 onder a BW.[25] De Richtlijn consumentenrechten[26] bevatte geen afzonderlijke informatieplicht ten aanzien van de compabiliteit van de digitale inhoud. Uit de Leidraad 2014 wordt duidelijk dat de compabiliteit van de digitale inhoud destijds werd begrepen onder de term 'interoperabiliteit' van de digitale inhoud.[27] Opmerkelijk is bovendien dat de Richtlijn consumentenrechten, en daarmee art. 6:230l en art. 6:230m lid 1 BW, geen afzonderlijke bepalingen bevatte over de functionaliteit, de compabiliteit en de interoperabiliteit van zaken met digitale elementen en van digitale diensten. De informatie daarover moet dus worden begrepen onder de meeromvattende term 'voornaamste kenmerken van de zaken of diensten' als bedoeld in art. 6:230l onder a en art. 6:230m lid 1 onder a BW.[28]

Met de inwerkingtreding van de Implementatiewet richtlijn modernisering consumentenbescherming bevatten art. 6:230l onder g en h en art. 6:230m lid 1 onder r en s BW een afzonderlijke informatieplicht ten aanzien de functionaliteit, compatibiliteit en interoperabiliteit van een zaak met digitale elementen, digitale inhoud of een digitale dienst. Deze informatieplichten dienen ertoe de consument te informeren over wat hij ten aanzien van de functionaliteit, interoperabiliteit en compatibiliteit mag verwachten van het domotica-apparaat. Het gaat daarbij om essentiële informatie die de gemiddelde consument nodig heeft om een geïnformeerde beslissing te kunnen nemen over het aanschaffen van het product. Tot 27 april 2022 behoorde, zoals gezegd, de informatie over de functionaliteit, compatibiliteit en interoperabiliteit van zaken met digitale elementen tot de 'voornaamste kenmerken van de zaken of diensten' in de zin van art. 6:230l onder a en art. 6:230m lid 1 onder a BW behoorde. Nu uit de parlementaire geschiedenis van de Implementatiewet niet blijkt dat de wetgever heeft beoogd op dit punt te breken met het tot dan toe geldende recht, is aannemelijk dat de verplichting voor de rechter tot ambtshalve toetsing en, zo nodig, algehele of gedeeltelijke vernietiging van de overeenkomst, zoals die door de Hoge Raad onder het tot 27 april 2022 geldende recht heeft geformuleerd voor op afstand of buiten verkoopruimte gesloten overeenkomsten, óók geldt ten aanzien van de informatie over de functionaliteit, compatibiliteit en interoperabiliteit van de domotica-apparaten. Ook hier zal bovendien sprake zijn van een misleidende omissie indien de informatie niet wordt verstrekt.[29]

2.1.3 Conformiteit en compatibiliteit, functionaliteit en interoperabiliteit

Art. 6:230n lid 2 BW brengt mee dat alle informatie die door de verkoper is verstrekt over de compatibiliteit, functionaliteit en interoperabiliteit van het domotica-apparaat deel uitmaakt van de overeenkomst, zodat de consument ook mag vertrouwen op deze informatie. Wanneer de digitale elementen van het domotica-apparaat niet overeenstemmen met de verstrekte informatie, is sprake van non-conformiteit overeenkomstig art. 7:18 BW. Art. 7:18 lid 1 onder a BW bepaalt in dit verband dat de

---

[25] Zie ook [24].

[26] Richtlijn 2011/83/EU, *Pub. EU* 2011, L 304/64.

[27] Zie Leidraad 2014 [3, p. 76] Zie in dit verband ook het hierboven genoemde voorbeeld uit de parlementaire geschiedenis van de implementatiewet van de Moderniseringsrichtlijn, waar de begrippen nog door elkaar lijken te lopen.

[28] Vgl. ook [24].

[29] Opgemerkt wordt dat art. 6:193f BW niet is aangepast aan de implementatie van de Moderniseringsrichtlijn, maar dat ook op dit punt niet is gebleken dat de wetgever heeft beoogd te breken met het tot dan toe geldende recht.

geleverde zaak moet voldoen aan de overeengekomen kenmerken ten aanzien van onder meer de functionaliteit, compatibiliteit en interoperabiliteit. Lid 2 onder d voegt daaraan toe dat de zaak ook de kenmerken moet bezitten ter zake van onder meer functionaliteit, compatibiliteit en beveiliging, die normaal zijn voor hetzelfde type zaken en die de koper redelijkerwijs mag verwachten.

Opmerkelijk is dat de begrippen compatibiliteit, functionaliteit en interoperabiliteit óók worden gedefinieerd in art. 7:5 lid 1 onder f, e, en g BW, maar dan steeds betrekking hebben op het vermogen van de *zaak* (al dan niet met digitale elementen) om zijn functies te vervullen en om te functioneren met andere hard- en software. Dat betekent dat bij de toepassing van de conformiteitscriteria van art. 7:18 BW tevens moet worden gekeken naar de gebruiksmogelijkheden van de gehele zaak en naar de mogelijkheid van die zaak om te interageren met andere zaken of digitale inhoud. De betekenis van de begrippen compatibiliteit, functionaliteit en interoperabiliteit verschilt dus enigszins tussen enerzijds de regels over de informatieplichten in art. 6:230l en art. 6:230m lid 1 BW, en anderzijds de regels over conformiteit in art. 7:18 BW.

In het kader van de conformiteit wordt onder de *functionaliteit* van de zaak verstaan het vermogen van de zaak om zijn functies te vervullen met betrekking tot het doel ervan (art. 7:5 lid 1 onder f BW). Deze bepaling heeft niet alleen betrekking op zaken met digitale elementen, maar geldt in beginsel ten aanzien van alle zaken. De functionaliteit van de in het domotica-apparaat verwerkte digitale inhoud (in de zin van art. 6:230g lid 1 onder x BW) bepaalt mede de wijze waarop het domotica-apparaat kan worden gebruikt, en bepaalt daarmee mede de functionaliteit van dat apparaat. Er bestaat echter een duidelijke samenhang tussen de informatieplichten van art. 6:230l onder g en art. 6:230m lid onder r BW en de conformiteit van de geleverde zaak in de zin van art. 7:18 BW: indien de verkoper van een domotica-apparaat zijn informatieplicht schendt, mag de consument verwachten dat het apparaat geschikt is voor normaal gebruik en dat het de functionaliteiten heeft die hij van een dergelijk apparaat mag verwachten. Dat betekent in het bijzonder dat hij niet behoeft te verwachten dat het apparaat is voorzien van regiocodering of Digital Rights Management[30] als gevolg waarvan hij het niet overeenkomstig zijn normale functies kan gebruiken. De te verwachten functionaliteit kan ook voortvloeien uit de aard van het gekochte domotica-apparaat. Wanneer de consument een *spraakassistent* gebruikt, zoals Alexa (Amazon) of Siri (Apple), mag hij verwachten dat de software kan interageren met de consument en daartoe gebruik kan maken van de in het apparaat ingebouwde speaker en microfoon; voor zover het apparaat moet kunnen bewegen, zal de software er bovendien voor moeten zorgen dat de wieltjes van het apparaat in beweging worden gebracht. Wanneer het apparaat hierbij een relevante beperking heeft – het kan bijvoorbeeld alleen reageren op Engelstalige commando's maar 'verstaat' geen Nederlands, dan is sprake van non-conformiteit indien de consument daar niet voor contractsluiting op duidelijke en begrijpelijke wijze over is geïnformeerd overeenkomstig art. 6:230l onder g of art. 6:230m lid onder r BW.

Onder de *compatibiliteit* van de zaak wordt in het kader van art. 7:18 BW verstaan het vermogen van de zaak om te functioneren met hardware of software waarmee dergelijke zaken gewoonlijk worden gebruikt, zonder dat die zaken of hardware of software moeten worden omgezet (art. 7:5 lid 1 onder e BW). Ook hiervoor geldt dat de compabiliteit van de in het domotica-apparaat verwerkte digitale inhoud (in de zin van art. 6:230g lid 1

[30] *Digital Rights Management (DRM)* omvat technologieën waarmee auteursrechten kunnen worden beschermd door het gebruik en kopiëren van digitale media te beperken.

onder y BW) mede bepaalt wat de consument van het gebruik van de zaak mag verwachten.

Onder de *interoperabiliteit* van de digitale inhoud wordt in het kader van art. 7:18 BW verstaan 'het vermogen van zaken om te functioneren met hardware of software die verschilt van die waarmee zaken van hetzelfde type gewoonlijk worden gebruikt' (art. 7:5 lid 1 onder g BW). Het gaat hierbij onder meer om de mogelijkheid om te communiceren met andere apparaten. Hierbij kan worden gedacht aan de mogelijkheid voor een 'slimme' wasmachine om te communiceren met een wasdroger. Een ander voorbeeld is de mogelijkheid om muziekbestanden over te brengen van of naar een andere drager.[31]

2.1.4 Precontractuele informatieplicht over updates

Updates kunnen ervoor zorgen dat de functionaliteit van de zaak wordt uitgebreid, dat de zaak (zonder dat deze hiervoor door de consument moet worden teruggebracht) aan technische ontwikkelingen kan worden aangepast, dat verbeteringen kunnen worden doorgevoerd, en dat de zaak met digitale elementen wordt beschermd tegen nieuwe beveiligingsdreigingen.[32] Wanneer geen updates worden geleverd, kunnen geen uitbreidingen, verbeteringen en aanpassingen van de zaak met digitale elementen worden doorgevoerd. Bovendien staat de zaak mogelijk bloot aan beveiligingsdreigingen. Dit maakt dat de zaak niet langer veilig kan worden gebruikt, of dat de zaak dusdanig verouderd is dat hij niet langer bruikbaar is. Daarvan is bijvoorbeeld sprake indien de zaak met digitale elementen niet langer kan communiceren met de hardware en software waarmee dergelijke zaken gewoonlijk worden gebruikt, waardoor functionaliteiten niet langer beschikbaar zijn en/of de zaak niet meer compatibel is met andere hardware of software.

Informatie over het updatebeleid – in het bijzonder over welke updates de consument mag verwachten en gedurende welke periode hij die verwachtingen mag hebben – is voor de gemiddelde consument essentiële informatie. Het updatebeleid behoort bij zaken met digitale elementen daarom tot de belangrijkste kenmerken waarover de consument voor contractsluiting dient te worden geïnformeerd. Volgens de Europese Commissie valt informatie ten aanzien van het updatebeleid onder de informatieplicht over de functionaliteit van (de digitale elementen van) het domotica-apparaat (art. 6:230l onder g en art. 6:230m lid onder r BW).[33] Wanneer dergelijke informatie niet voor contractsluiting is verstrekt, is dat een misleidende omissie in de zin van art. 6:193d BW. Dat betekent dat als de concrete consument die het domotica-apparaat heeft gekocht mogelijk een andere beslissing zou hebben genomen over de aanschaf van het domotica-apparaat indien de informatie wel (op duidelijke en begrijpelijke wijze) zou zijn verstrekt, hij de overeenkomst kan vernietigen, hetzij analoog aan het arrest van de Hoge Raad op de voet van art. 3:40 lid 2 BW, hetzij op grond van art. 6:193j lid 3 BW.

2.1.5 Conformiteit en updateverplichting

Na levering is de verkoper uiteraard gehouden het updatebeleid ook uit te voeren overeenkomstig de verstrekte informatie, die immers deel is gaan uitmaken van de

---

[31] *Kamerstukken II* 2021/22, 35 940, nr. 3, p. 27 en overweging 27 in de preambule bij de Richtlijn verkoop goederen (Richtlijn (EU) 2019/771, *PubEU* 2019, L 136/28).

[32] *Kamerstukken II* 2020/21, 35 734, nr. 3, p. 32-33. Overigens kunnen updates ook essentieel zijn om de functionaliteit van de zaak zelfs maar te *behouden,* of juist worden gebruikt om de functionaliteit te verminderen.

[33] Zie Leidraad 2014 [3, p. 77]. In de Richtsnoeren 2021 [2, p. 35], laat de Europese Commissie in het midden of het in dit verband gaat om functionaliteit, interoperabiliteit of compabiliteit.

overeenkomst (art. 6:230n lid 2 BW), zo vloeit voort uit art. 7:18 lid 1 onder d BW. Maar ook indien geen of slechts beperkte informatie is verstrekt over het updatebeleid, kan de verkoper gehouden updates te leveren. In dit verband moet worden gewezen op de in art. 7:18 lid 4 BW opgenomen updateverplichting. Deze verplichting vormt een van de belangrijkste onderdelen van de nieuwe regeling voor de consumentenkoop (en voor de overeenkomstige regeling voor overeenkomsten tot levering van digitale inhoud en digitale diensten).[34] Deze bepaling brengt mee dat ook zonder contractuele afspraak de verkoper ervoor dient te zorgen dat de updates die nodig zijn om de afgeleverde zaak aan de overeenkomst te laten beantwoorden, aan de koper worden gemeld en geleverd gedurende de periode die de consument redelijkerwijs kan verwachten gezien de aard en het doel van de zaak en de digitale elementen, en rekening houdend met de omstandigheden en de aard van de overeenkomst als de koop voorziet in levering van de digitale inhoud of digitale dienst.

De verkoper dient de consument er bovendien over te informeren dat en hoe hij de update moet installeren op de roerende zaak waarin de digitale inhoud of dienst is verwerkt, en wat de gevolgen zijn als de consument de update niet installeert (lid 5). Het gaat hier derhalve om een door de verkoper na te komen (post)contractuele informatieverplichting.

De updateverplichting geldt echter niet indien de consument er voor contractsluiting uitdrukkelijk van in kennis is gesteld dat een specifiek kenmerk van de zaak afwijkt van wat de consument normaal zou mogen verwachten, en de consument die afwijking bij het sluiten van de overeenkomst uitdrukkelijk en afzonderlijk heeft aanvaard (lid 6). Dat kan betekenen dat partijen *bij* contractsluiting uitdrukkelijk overeenkomen dat geen, of slechts gedurende beperkte tijd, updates worden geleverd. De hiervoor genoemde precontractuele informatieplicht over het updatebeleid houdt in dat geval dus in dat de consument er *voor* contractsluiting uitdrukkelijk over wordt geïnformeerd dat hij juist geen updates mag verwachten. Wanneer de consument vervolgens uitdrukkelijk en afzonderlijk te kennen geeft dat hij akkoord gaat met het niet leveren van updates, mag hij deze op grond van art. 7:18 BW ook niet verwachten. Is aan een van de vereisten van art. 7:18 lid 6 BW niet voldaan, geldt de updateverplichting echter in ongewijzigde vorm.

2.1.6 Beperkingen aan het gebruik en conformiteit

Een bijzonder kenmerk van zaken met digitale elementen is dat de verkoper wel de eigendom van de zaak kan verschaffen, maar niet (alle) intellectuele eigendomsrechten die aan de digitale inhoud verbonden zijn. In ieder geval een deel van deze intellectuele eigendomsrechten, de morele rechten, zijn verbonden aan de persoon van de ontwikkelaar (maker) van de digitale inhoud (of diens werkgever) en daarom niet-overdraagbaar.[35] Dat brengt mee dat de ontwikkelaar deze rechten niet kan vervreemden. Niet aan de opdrachtgever en niet aan de verkoper. De verkoper kan deze intellectuele eigendomsrechten dus ook niet hebben verworven. Op zijn beurt kan de verkoper deze intellectuele eigendomsrechten (dus) ook niet overdragen. De consument mag een dergelijke overdracht ook niet verwachten. Wél mag hij verwachten dat hij de zaak met digitale elementen overeenkomstig hun bestemming kan gebruiken, tenzij hij er vóór contractsluiting uitdrukkelijk over is geïnformeerd dat hij de zaak met digitale elementen,

---

[34] In deze zin de Minister voor Rechtsbescherming en de Staatssecretaris van Economische Zaken en Klimaat in de memorie van toelichting bij het wetsvoorstel, *Kamerstukken II* 2020/21, 35 734, nr. 3, p. 19.

[35] Het gaat hier om bepaalde morele rechten zoals het recht om op te treden tegen verminkingen. Hier wordt niet ingegaan op de eventuele mogelijkheid om octrooirechten te vestigen.

anders dan hij anders had mogen verwachten, niet voor een specifiek te noemen doeleinde kan gebruiken en hij die afwijking bij het sluiten van de overeenkomst uitdrukkelijk en afzonderlijk heeft aanvaard (art. 7:18 lid 6 BW, de 'dubbele uitdrukkelijkheidstoets'). Op deze wijze kan de verkoper de consument informeren over een specifieke beperking van de gebruiksmogelijkheden van de zaak met digitale elementen die voortvloeit uit de intellectuele eigendomsrechten van de verkoper. Wordt de consument niet op een dergelijke specifieke beperking gewezen, dan behoeft hij een dergelijke beperking van de normale gebruiksmogelijkheden van de digitale inhoud ook niet te verwachten.

2.1.7 Beperkingen in de vorm van shrinkwrap-licenties

Bij domotica-apparaten komt het regelmatig voor dat beperkingen in de verwachtingen die een consument van de zaak mag hebben, zijn opgenomen in algemene voorwaarden (of: gebruiksvoorwaarden) die afkomstig zijn van de fabrikant. Vaak maakt de fabrikant daarbij gebruik van zogenaamde *shrinkwrap*-licenties, waarbij de algemene voorwaarden zijn opgenomen in de verpakking van het apparaat. Voor zover de verkoper de consument niet vooraf heeft geïnformeerd over het gebruik van de algemene voorwaarden en deze niet zichtbaar zijn vóór contractsluiting, is de consument niet gebonden aan de algemene voorwaarden van de producent. Daarbij verdient opmerking dat de consument ook geen afzonderlijke overeenkomst heeft gesloten met de fabrikant als deze niet de verkoper was. Uit het enkele feit dat de consument het domotica-apparaat gebruikt overeenkomstig de daaraan door de producent gegeven bestemming kan geen instemming met het sluiten van een overeenkomst met die producent worden afgeleid.

Dat kan echter anders zijn als de verkoper de consument vóór contractsluiting heeft geïnformeerd over het bestaan van de algemene voorwaarden en hij de consument in de gelegenheid heeft gesteld om kennis te nemen van die algemene voorwaarden.[36] [4] In een dergelijk geval bedingt de verkoper ten gunste van de fabrikant van het domotica-apparaat de toepasselijkheid van diens algemene voorwaarden, welk derdenbeding door de fabrikant op de voet van artikel 6:253 BW zal worden aanvaard. In een dergelijk geval zal met het verbreken van de *shrinkwrap* een driepartijenovereenkomst tot stand komen, waarbij in de verhouding tussen de consument en de fabrikant ook de algemene voorwaarden van de fabrikant van toepassing zijn. Op deze algemene voorwaarden is wél de regeling van afd. 6.5.3 BW van toepassing, zodat onredelijk bezwarende bedingen kunnen worden vernietigd op de voet van art. 6:233 onder a BW. Bovendien geldt dat voor zover de algemene voorwaarden van de fabrikant gebruiksbeperkingen bevatten die de consument op grond van de koopovereenkomst niet behoefde te verwachten omdat niet voldaan is aan de dubbele uitdrukkelijkheidstoets van art. 7:18 lid 6 BW, deze algemene voorwaarden een afwijking vormen van de wettelijke regels van de consumentenkoop en zij daarmee op de voet van art. 7:6 lid 1 BW vernietigbaar zijn.

2.1.8 Beperkingen in de vorm van clickwrap-licenties

In de praktijk komt het ook regelmatig voor dat de algemene voorwaarden van de fabrikant niet door middel van een *shrinkwrap*-licentie, maar door middel van een *clickwrap*-licentie van toepassing worden verklaard. Ook hier geldt dat de algemene voorwaarden van de fabrikant dan van toepassing moeten worden op grond van een ten gunste van hem in de koopovereenkomst opgenomen derdenbeding, dat door de fabrikant wordt aanvaard. In een dergelijk geval wordt de consument, wanneer hij het domotica-apparaat klaar wil maken voor gebruik en hij daartoe de vooraf-geïnstalleerde of te downloaden digitale inhoud wil

[36] Zie nader [4] nr. 65. In deze zin ook [25, p. 129].

activeren, gedwongen om de toepasselijkheid van algemene voorwaarden te aanvaarden voordat hij de digitale inhoud kan activeren. Bij *clickwrap*-licenties wordt de aanvaarding van de toepasselijkheid van de algemene voorwaarden niet bij de bestelling, maar pas voorafgaande aan het downloaden van de digitale inhoud of de installatie daarvan gevraagd. Wanneer niet vóór contractsluiting door de verkoper is gewezen op het gebruik van de algemene voorwaarden door de fabrikant van het domotica-apparaat, is de toepasselijk verklaring van de algemene voorwaarden voorafgaande aan de download of de installatie van de digitale inhoud simpelweg te laat om tot toepasselijkheid van de algemene voorwaarden te kunnen leiden. Uit het enkele feit dat de consument op een later moment lijkt in te stemmen met de toepasselijkheid van de algemene voorwaarden kan de toepasselijkheid niet worden afgeleid, nu de consument geen mogelijkheid heeft om de – al aangeschafte en veelal reeds betaalde – digitale inhoud te downloaden of te activeren zonder akkoord te gaan met het 'wijzigingsvoorstel'.[37] Daaraan doet ook niet af dat de algemene voorwaarden van de fabrikant mogelijk op diens website zijn gepubliceerd. Uit rechtspraak van de Hoge Raad volgt immers dat van de consument niet mag worden verwacht dat hij deze algemene voorwaarden zelf vóór sluiting van de koopovereenkomst opzoekt, zelfs niet indien de verkoper de consument vóór contractsluiting heeft gewezen op de vindplaats van de algemene voorwaarden: in een dergelijk geval zijn de algemene voorwaarden van de fabrikant wel van toepassing geworden op de overeenkomst, maar zijn deze vernietigbaar op grond van art. 6:233 onder b BW.[38]

Voor zover geoordeeld zou worden dat een consument met het aanvinken van een vakje *alsnog* instemt met de toepasselijkheid van de algemene voorwaarden van de fabrikant, is verdedigbaar dat een dergelijke (aanvullende) overeenkomst vernietigbaar is wegens misbruik van omstandigheden (art. 3:44 lid 1 jo. lid 4 BW) dan wel een agressieve handelspraktijk (art. 6:193h lid 1 jo. 193j lid 3 BW), nu de consument feitelijk wordt gedwongen akkoord te gaan met het sluiten van een overeenkomst om het domotica-apparaat te kunnen gebruiken dat hij al gekocht heeft, terwijl de fabrikant geen recht kan doen gelden op de toepassing van de licentievoorwaarden. Voor zover de consument het domotica-apparaat *feitelijk* niet kan gebruiken zonder de (aanvullende) overeenkomst met de fabrikant te sluiten, is ook de koopovereenkomst met de verkoper gesloten onder invloed van een oneerlijke handelspraktijk, meer in het bijzonder een misleidende omissie, aangezien essentiële informatie over de geschiktheid van het gebruik van het apparaat niet is verstrekt.[39] Dat betekent dat ook de koopovereenkomst in voorkomend geval door de consument kan worden vernietigd. Uiteraard zal de consument de intellectuele eigendomsrechten van de producent moeten respecteren, maar dat geldt ook zonder dat de consument licentievoorwaarden heeft moeten aanvaarden.[40]

2.1.9 Wijzigingen van digitale inhoud

In de door de fabrikant van domotica-apparaten gehanteerde algemene voorwaarden is soms opgenomen dat functionaliteiten of ander eigenschappen kunnen worden gewijzigd of verwijderd.

Voor zover de digitale inhoud moet worden gewijzigd om ervoor te zorgen dat het domotica-apparaat aan de overeenkomst blijft beantwoorden, is een dergelijke wijziging

---

[37] Vgl. [4], nr. 66a.

[38] Hoge Raad 11 februari 2011, ECLI:NL:HR:2011:BO7108, *NJ* 2011/571 (First Data B.V./KPN Hotspots Schiphol B.V.).

[39] Vgl. art. 6:193d lid 2 jo. 193f onder b BW.

[40] Vgl. [4], nr. 66a.

ook zonder daartoe strekkend beding toegestaan. Op de verkoper rust immers de verplichting om updates te leveren die ervoor kunnen zorgen dat het domotica-apparaat aan de overeenkomst blijft beantwoorden (art. 7:18 lid 4 BW).

Daarbij moet echter worden opgemerkt dat het verminderen of verwijderen van een bestaande functionaliteit al snel zal meebrengen dat het domotica-apparaat *daardoor* niet meer aan de overeenkomst beantwoordt. Na een dergelijke wijziging beschikt het domotica-apparaat immers niet (meer) over de functionaliteiten die de consument daarvan redelijkerwijs mag verwachten, gelet op de aard van de zaak en de functionaliteit die voor hetzelfde type apparaat normaal is (art. 7:18 lid 2 onder d BW).

Een verplichting tot levering van updates geldt niet voor zover deze *niet* nodig zijn om ervoor te zorgen dat het domotica-apparaat aan de overeenkomst blijft beantwoorden. Omgekeerd geldt dat de consument, zonder daartoe strekkend beding, ook niet gehouden is een dergelijke update te accepteren, en dat een door de fabrikant opgedrongen niet-noodzakelijke update een inbreuk vormt op het eigendomsrecht van de consument, in het bijzonder als hierdoor de functionaliteit van het domotica-apparaat zou worden verminderd of een functionaliteit geheel zou worden verwijderd. Daarmee zou de fabrikant onrechtmatig handelen. Bovendien zou sprake zijn van een agressieve, en daarmee oneerlijke, handelspraktijk in de zin van art. 6:193h jo. 193i onder c BW indien de fabrikant bij herhaling blijft aandringen op het downloaden en installeren van de update. Daarvan is eveneens sprake indien de fabrikant ervoor zorgt dat de update automatisch wordt geïnstalleerd, ongeacht de door de consument gekozen update-instellingen, of hij ervoor zorgt dat het domotica-apparaat niet meer functioneert voordat een update wordt geïnstalleerd. Ook daaruit zou volgen dat de fabrikant onrechtmatig handelt (art. 6:193b lid 1 en 3 BW).

Wanneer de algemene voorwaarden van de fabrikant wél een daartoe strekkend wijzigingsbeding bevatten, moet voorop worden gesteld dat een dergelijk beding alleen zou *kunnen* leiden tot een geldige rechtsgrond voor wijziging van de digitale inhoud indien het beding deel is gaan uitmaken van de consumentenkoopovereenkomst of van een afzonderlijke overeenkomst tussen de fabrikant en de consument. Dergelijke bedingen zijn echter in strijd met de wet en daarmee vernietigbaar. De juridische constructie op basis waarvan deze conclusie wordt bereikt, hangt af van de juridische relatie tussen de consument en de fabrikant.

Ervan uitgaand dat de digitale inhoud noodzakelijk is om gebruik te kunnen maken van het door de consument gekochte domotica-apparaat, is de digitale inhoud te zien als een toebehoren in de zin van art. 7:9 lid 1 BW die op grond van de koopovereenkomst door de verkoper ter beschikking van de consument moet worden gesteld. Zoals hierboven is aangegeven, worden de algemene voorwaarden van de fabrikant van het domotica-apparaat alleen dan deel van de koopovereenkomst als de verkoper de consument hier voor contractsluiting over heeft geïnformeerd en de consument de toepasselijkheid daarvan heeft aanvaard.

a. Voor zover zou worden geoordeeld dat de fabrikant met de aanvaarding van het in zijn belang door de verkoper opgenomen derdenbeding is toegetreden tot de consumentenkoopovereenkomst, geldt dat de beoordeling van het wijzigingsbeding moet worden getoetst aan de regels voor de consumentenkoop.
b. Voor zover zou worden geoordeeld dat met de aanvaarding van het derdenbeding een *afzonderlijke* overeenkomst tot levering van digitale inhoud zou zijn gesloten, zou de wettelijke regeling van titel 7.1AA BW van toepassing zijn.

Beide regelingen leiden evenwel tot dezelfde uitkomst.

Ad a. De wettelijke regeling van de consumentenkoop bevat geen uitdrukkelijke regeling voor de mogelijkheid tot wijziging van de digitale inhoud, afgezien van de levering van updates die nodig zijn om te bewerkstelligen dat het domotica-apparaat aan de overeenkomst blijft beantwoorden.[41] Dat suggereert dat een dergelijke wijziging niet is toegestaan, tenzij de functionaliteit, compatibiliteit en interoperabiliteit van het apparaat en de andere eigenschappen van het apparaat niet worden verminderd door de wijziging, of de wijziging slechts leidt tot extra functionaliteiten. Als de wijziging er bijvoorbeeld toe leidt dat de functionaliteit van het apparaat wordt verminderd, voldoet het domotica-apparaat niet aan de functionaliteit die de consument redelijkerwijs van het domotica-apparaat mag verwachten, gelet op de aard van de zaak en de functionaliteit die voor hetzelfde type apparaat normaal is (art. 7:18 lid 2 onder d BW). Daarbij geldt dat het moment van contractsluiting het moment is waarop wordt bepaald over welke functionaliteiten het domotica-apparaat dient te beschikken. Omstandigheden die zich nadien hebben voorgedaan – zoals de latere mededeling van de verkoper dat de zaak niet voor het door de consument gewenste doel kan worden gebruikt –, kunnen geen afbreuk doen aan de gerechtvaardigde verwachtingen die de consument van het domotica-apparaat mag hebben.[42] Wanneer het wijzigingsbeding ertoe leidt dat de fabrikant van het domotica-apparaat bevoegd zou zijn tot het verminderen of verwijderen van functionaliteit of andere eigenschappen van het apparaat door middel van wijziging van de digitale inhoud, wijkt het beding ten nadele van de consument af van de wettelijke regeling van de consumentenkoop. Een dergelijke afwijking is in strijd met dwingend recht en daarmee vernietigbaar (art. 7:6 jo. 3:40 lid 2 BW).

Ad b. Art. 7:50al BW biedt voor overeenkomsten tot levering van digitale inhoud of digitale diensten wél een mogelijkheid tot wijziging van de digitale inhoud of dienst die niet noodzakelijk is om te bewerkstelligen dat de digitale inhoud aan de overeenkomst blijft beantwoorden. Art. 7:50al lid 1 BW stelt daarvoor wel enkele eisen:

- In de overeenkomst moet een wijzigingsbeding zijn opgenomen;
- Voor de wijziging moet een gegronde reden bestaan, welke ook in het wijzigingsbeding moet zijn genoemd;
- De wijziging moet worden uitgevoerd zonder dat hiervoor aanvullende kosten aan de consument in rekening worden gebracht.

Voor zover de wijziging negatieve gevolgen heeft voor de toegang van de consument tot de digitale inhoud of dienst of voor het gebruik daarvan, dient de consument bovendien vooraf te zijn geïnformeerd over de wijziging én van de mogelijkheid om de overeenkomst te ontbinden óf van de mogelijkheid om de digitale inhoud of digitale dienst zonder wijziging te behouden en de digitale inhoud of digitale dienst daarmee blijft beantwoorden aan de overeenkomst.[43] Uit dit samenstel van voorwaarden kan worden afgeleid dat ook bij een afzonderlijke overeenkomst tot levering van digitale inhoud of een digitale dienst de handelaar niet mag overgaan tot een vermindering van de functionaliteit van de digitale inhoud of dienst of het verwijderen van een functionaliteit, zelfs niet indien hij een daartoe strekkend beding in de overeenkomst zou hebben opgenomen. Een beding waarmee hij een dergelijke bevoegdheid toch zou hebben bedongen, is in strijd met dwingend recht (art. 7:50ap lid 1 BW) en daarmee eveneens op grond van art. 3:40 lid 2 BW vernietigbaar.

---

[41] Vgl. art. 7:18 lid 4 BW.

[42] Vgl. [26], nr. 31.

[43] Vgl. art. 7:50al lid 1 onder d, lid 2 en lid 4 BW.

2.2 Juridisch kader: richtlijn radioapparatuur

Voor zover relevant bespreken we hier de Richtlijn radioapparatuur[44] (hierna: Radiorichtlijn) en de onderliggende regelgeving. De Radiorichtlijn bevat regelgeving voor het op de markt brengen van radioapparatuur en bevat zowel eisen met betrekking tot zaken als fysieke veiligheid als eisen met betrekking tot bescherming van de gezondheid, de elektromagnetische compatibiliteit en het efficiënte spectrumgebruik. Daarnaast bevat het optionele eisen waarvan enkele aan digitale veiligheid zijn gerelateerd. De voor dit onderzoek relevante bepalingen zijn in Nederland geïmplementeerd in de Telecommunicatiewet, het Besluit radioapparaten en de Regeling radioapparaten.

Naast essentiële eisen bevat de Radiorichtlijn procedurele regels en informatieverplichtingen richting lidstaten die buiten de scope van dit onderzoek vallen. In deze paragraaf bespreken we enkel de eisen die aan apparatuur worden gesteld en de informatieverplichtingen richting consumenten. Ook hiervan is de relevantie echter beperkt voor dit onderzoek. Zo is in oktober 2021 een gedelegeerde verordening[45] tot aanvulling van de Radiorichtlijn aangenomen. De bepalingen hierin zijn relevant voor dit onderzoek, en worden hieronder besproken, maar de verplichtingen worden pas in augustus 2024 van kracht.

2.2.1 Definities

Radioapparatuur wordt gedefinieerd als 'elektrisch of elektronisch product dat doelbewust radiogolven[46] uitzendt en/of ontvangt ten behoeve van radiocommunicatie[47] en/of radiodeterminatie[48], of elektrisch of elektronisch product dat moet worden aangevuld met een accessoire, zoals een antenne, om doelbewust radiogolven te kunnen uitzenden en/of ontvangen ten behoeve van radiocommunicatie en/of radiodeterminatie' (art. 2 lid 1 van de Radiorichtlijn).

2.2.2 Eisen aan apparatuur

Artikel 3 van de Radiorichtlijn bevat de essentiële eisen die aan radioapparatuur worden gesteld en waarnaar wordt verwezen in de Telecommunicatiewet (art. 10.9) en het Besluit radioapparaten (art. 3). De eerste twee leden zijn op vrijwel alle radioapparatuur van toepassing, maar zien met name op de bescherming van gezondheid en effectief en efficiënt gebruik van het radiospectrum. Zij zijn voor dit onderzoek niet relevant. Het derde lid bevat wel een aantal bepalingen die voor dit onderzoek van belang zijn, maar de eisen die hierin zijn opgenomen zijn niet automatisch van toepassing; via gedelegeerde

---

[44] Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG.

[45] Gedelegeerde verordening (EU) 2022/30 van de commissie van 29 oktober 2021 tot aanvulling van Richtlijn 2014/53/EU van het Europees Parlement en de Raad met betrekking tot de toepassing van de essentiële eisen als bedoeld in artikel 3, lid 3, punten d), e) en f), van die richtlijn.

[46] *Radiogolven*: elektromagnetische golven met frequenties van lager dan 3.000 GHz, die zich in de ruimte voortplanten zonder kunstmatige geleider (art. 2 lid 4 van de Radiorichtlijn).

[47] *Radiocommunicatie*: communicatie door middel van radiogolven (art. 2 lid 2 van de Radiorichtlijn).

[48] *Radiodeterminatie*: het vaststellen van de positie, snelheid en/of andere kenmerken van een object of het verkrijgen van informatie over deze parameters door middel van de voortplantingseigenschappen van radiogolven (art. 2 lid 3 van de Radiorichtlijn).

handelingen kunnen categorieën radioapparatuur worden gespecificeerd waarop de verschillende eisen van toepassing zijn (art. 3 lid 3 van de Radiorichtlijn).

Er is een aantal gedelegeerde verordeningen aangenomen in het kader van artikel 3 lid 3 van de Radiorichtlijn. Hiervan is er slechts één van belang voor domotica-apparaten, maar de eisen gelden pas vanaf 1 augustus 2024. Hieronder is aangegeven welke eisen voor welke categorieën apparaten van toepassing worden:

Eis: radioapparatuur schaadt het netwerk of de werking ervan niet en maakt evenmin misbruik van de netwerkmiddelen waardoor een onaanvaardbare achteruitgang van de dienst wordt veroorzaakt (art. 3 lid 3 onder d van de Radiorichtlijn)

Deze eis is per 1 augustus 2024 van toepassing op 'radioapparatuur die in staat is zelfstandig via het internet te communiceren, ongeacht of dit rechtstreeks of via andere apparatuur geschiedt' (hierna: 'met internet verbonden radioapparatuur').[49] Deze eis zal dus van toepassing zijn op veel domotica-apparaten.

Eis: radioapparatuur bevat beveiligingen om de bescherming van de persoonsgegevens en de privacy van de gebruiker en de abonnee te waarborgen (art. 3 lid 3 onder e van de Radiorichtlijn)

Deze eis is per 1 augustus 2024 van toepassing op veel domotica apparaten, het gaat namelijk om:[50]

a. met internet verbonden radioapparatuur;
b. bepaalde categorieën radioapparatuur, ook wanneer zij niet met internet verbonden zijn:
    a. radioapparatuur die ontworpen of bedoeld is om uitsluitend bij de kinderzorg te worden gebruikt (bijvoorbeeld 'slimme' babyfoons)
    b. radioapparatuur die onder Richtlijn 2009/48/EG valt (speelgoed)
    c. radioapparatuur die ontworpen of bestemd is om al dan niet uitsluitend te worden gedragen op, vastgemaakt aan of gehangen van:
        i. enig deel van het menselijk lichaam, met inbegrip van de kop, hals, romp, armen, handen, benen en voeten;
        ii. door mensen gedragen kleding, met inbegrip van hoofddeksels, handschoenen en schoeisel.

Eis: radioapparatuur ondersteunt bepaalde mogelijkheden die bescherming tegen fraude waarborgen (art. 3 lid 3 onder f Radiorichtlijn)

Deze eis is van per 1 augustus 2024 van toepassing op alle met internet verbonden radioapparatuur, als die apparatuur de houder of gebruiker in staat stelt geld, monetaire waarde of virtuele valuta[51] over te maken.[52] Hier kan bijvoorbeeld sprake van zijn indien een domotica-apparaat, zoals een smart-tv of hub, met een creditcard gekoppeld is.

---

[49] Gedelegeerde verordening (EU) 2022/30, art. 1 lid 1.

[50] Gedelegeerde verordening (EU) 2022/30, art. 1 lid 2.

[51] "Een digitale weergave van waarde die niet door een centrale bank of een overheid wordt uitgegeven of gegarandeerd, die niet noodzakelijk aan een wettelijk vastgestelde valuta is gekoppeld en die niet de juridische status van valuta of geld heeft, maar die door natuurlijke of rechtspersonen als ruilmiddel wordt aanvaard en die elektronisch kan worden overgedragen, opgeslagen en verhandeld." (Richtlijn (EU) 2019/713, art. 2 onder d.)

[52] Gedelegeerde verordening (EU) 2022/30, art. 1 lid 3.

2.2.3 Informatieverstrekking aan consumenten

Op basis van de Radiorichtlijn hebben fabrikanten een aantal informatieplichten richting consumenten, in de zin dat ze ervoor moeten zorgen dat hun apparatuur vergezeld gaat van bepaalde informatie. Zo moeten zij bijgevoegd bij de apparatuur informatie verschaffen over:

- Hun naam, handelsnaam of geregistreerde merknaam en contactadres (art. 10 lid 7 van de Radiorichtlijn).
- Instructies en veiligheidsinformatie die makkelijk te begrijpen zijn. De instructies bevatten de voor het beoogde gebruik van de radioapparatuur noodzakelijke informatie. Deze informatie omvat, in voorkomend geval, een beschrijving van de accessoires en onderdelen, met inbegrip van software, die het mogelijk maken dat de radioapparatuur functioneert zoals bedoeld (art. 10 lid 8 van de Radiorichtlijn).
- Indien het apparaat doelbewust radiogolven uitzendt (art. 10 lid 8 van de Radiorichtlijn):
    - De frequentieband(en) waarin de radioapparatuur functioneert;
    - Het maximaal radiofrequent vermogen uitgezonden in de frequentieband(en) waarin de radioapparatuur functioneert.
- Een kopie van de EU-conformiteitsverklaring of een vereenvoudigde EU-conformiteitsverklaring. Als een vereenvoudigde EU-conformiteitsverklaring wordt verstrekt, bevat deze het juiste internetadres waar de volledige tekst van de EU-conformiteitsverklaring te vinden is (art. 10 lid 9 van de Radiorichtlijn).

Importeurs en distributeurs hebben tot slot de verplichting om te controleren of aan bovenstaande informatieverplichtingen is voldaan, voordat zij deze in de handel brengen (art. 12 lid 2 en 13 lid 2 van de Radiorichtlijn).

3 Methode

In dit hoofdstuk beschrijven we de wijze waarop domotica-apparaten in dit onderzoek worden onderzocht. Het hoofdstuk is ingedeeld naar de fasen waaruit het onderzoek bestaat. Iedere fase bestaat uit een aantal testhandelingen, die we in dit hoofdstuk nader beschrijven. In paragraaf 3.10 beschrijven we tot slot hoe we omgaan met specifieke uitzonderingssituaties die zich gedurende het onderzoek zouden kunnen voordoen.

Fase	Onderzoeksstappen
1. Voorbereidende fase	3.1 Selectie onderzochte kenmerken 3.2 Apparaatselectie
2. Aankoopfase	3.3 Verzamelen van precontractueel verstrekte informatie 3.4 Monitoring informatievoorziening
3. Ingebruiknamefase	3.5 Ingebruikname 3.6 Analyse functionaliteit, compatibiliteit, interoperabiliteit, updatebeleid
4. Einde ingebruiknamefase	3.7 Analyse digitale veiligheid aan de hand van vereisten
5. Gebruiksfase (3 maanden)	3.8 Gebruik van het apparaat 3.9 Analyse veiligheid updatemethodiek 3.4 Monitoring informatievoorziening (*herhaling*)
6. Einde gebruiksfase	3.6 Analyse functionaliteit, compatibiliteit, interoperabiliteit, updatebeleid (*herhaling*) 3.7 Analyse digitale veiligheid aan de hand van vereisten (*herhaling*)

3.1 Selectie onderzochte kenmerken

In het onderzoek worden de eigenschappen van de apparaten gerelateerd aan functionaliteit, compatibiliteit, interoperabiliteit en het updatebeleid (hierna: FCIU) geanalyseerd. Het primaire doel hiervan is om te bepalen in hoeverre de FCIU-eigenschappen in de praktijk overeenkomen met de precontractuele informatie daarover, op moment van ingebruikname en gedurende de gebruiksperiode. Concreet betreft het onder andere de volgende aspecten, die invulling geven aan de begrippen zoals ze gedefinieerd zijn in het juridisch kader (zie par. 2.1.3 en 2.1.4):

- De set platforms[53] (veelal voor 'smart home' of spraakassistenten) die het apparaat ondersteunt;

[53] Met '*platform*' bedoelen we hier: dienst waar domotica-apparaten aan kunnen worden gekoppeld, en aanvullende functionaliteit levert (bijvoorbeeld het kunnen bedienen van een domotica-apparaat via een smartphone, het kunnen bedienen via een spraakassistent op een smartphone of slimme speaker, het kunnen programmeren van automatische schakelingen op basis van andere bronnen, et cetera).

- Standaarden die ondersteund worden (veelal draadloze, netwerk- en 'smart home'-standaarden) en waarmee gekoppeld zou kunnen worden met willekeurige andere apparaten, ook van andere merken, die ook de standaard ondersteunen;
- Standaarden voor draadloze connectiviteit die worden ondersteund en nodig zijn om het product te kunnen gebruiken zoals geadverteerd;
- De functies van het apparaat die afhankelijk zijn van de software op het apparaat;
- Op welke (mobiele) besturingssystemen en versies daarvan bijbehorende apps werken.

Deze aspecten zijn uitgewerkt naar concreet meetbare kenmerken die we in het vervolg 'FCIU-kenmerken' noemen.

Wijze van concretisering

De set door ons gecontroleerde eigenschappen is vastgesteld gegeven de middelen die beschikbaar waren voor dit onderzoek. Allereerst is een inventarisatie gemaakt van concreet meetbare kenmerken op gebied van FCIU op twee vergelijkingswebsites (Tweakers Pricewatch en Kieskeurig). Hierbij is gekeken naar de attributen waarop deze websites producten kunnen filteren, en de kenmerken die per product op productpagina's beschikbaar zijn. Er is niet gekeken naar de kenmerken die verkopers en fabrikanten op de website tonen. Op basis van de inventarisatie is een selectie gemaakt van kenmerken op basis van specifieke relevantie voor domotica-apparaten (een attribuut moet refereren aan een 'slimme' functie – een kenmerk als "materiaal wasmachinetrommel" is in het kader van dit onderzoek niet relevant). Daarnaast is gestreefd naar een evenwichtige verdeling over de verschillende kenmerken. De set kenmerken is daarna langs het juridisch kader gelegd, en tot slot afgestemd met de opdrachtgever.

Tabel 1 toont de voor dit onderzoek geselecteerde concrete FCIU-kenmerken.

Tabel 1 Overzicht van de in dit onderzoek geanalyseerde concrete FCIU-kenmerken

Nr.	Kenmerk	Format/voorbeeld
1	Minimumversie Android (smartphone) van bijbehorende app	Versienummer (x.y) en eventuele verdere beperkingen
2	Minimumversie iOS/iPadOS van bijbehorende app	Versienummer (x.y) en eventuele verdere beperkingen
3	Ondersteunde Wi-Fi-technologieën	802.11a/b/g/n/ac/ax, Wi-Fi-x
4	Ondersteunde Wi-Fi-frequenties	2,4GHz, 5GHz, etc.
5	Gegarandeerde termijn voor volledige updates	x jaar
6	Gegarandeerde termijn voor beveiligingsupdates	x jaar
7	Ondersteunde smarthome-platformen, spraakassistenten	Amazon Alexa, Apple HomeKit, Google Nest, Philips Hue, IKEA Tradfri, Domoticz, Home Assistant, etc.
8	Ondersteunde opslagmedia	SDXC, etc.
9	Ondersteunde Wi-Fi-beveiligingsmethoden	WPA, WPA2, WPA3, etc.

Nr.	Kenmerk	Format/voorbeeld
10	Ondersteunde bedrade interfaces	OpenTherm, modulerende CV-ketel, etc.
11	Clouddienst nodig voor functies	Bijv. online kijken babyfooncamera
12	Internet nodig voor functies	Lijst met functies
13	Compatibele ZigBee-versie(s)	Minimumversie (x.y) en eventueel variant
14	Compatibele Thread-versie(s)	Minimumversie (x.y) en eventueel variant
15	Compatibele 6LoWPAN-versie(s)	Minimumversie (x.y) en eventueel variant
16	Updates worden automatisch opgehaald en geïnstalleerd	Ja/nee, interval, wanneer wordt dit aangeboden

Volledige updates

In bovenstaande bedoelen we met het begrip "*volledige update*" een update die noodzakelijk is om het product conform (in de betekenis van het consumentenrecht) te houden. Zie Artikel 7:18 lid 4 BW: *"4. Bij een zaak met digitale elementen zorgt de verkoper ervoor dat de updates, waaronder beveiligingsupdates, die nodig zijn om te bewerkstelligen dat de afgeleverde zaak aan de overeenkomst beantwoordt, aan de koper worden gemeld en geleverd gedurende de periode die de koper redelijkerwijs kan verwachten, gezien de aard en het doel van de zaak en de digitale elementen, en rekening houdend met de omstandigheden en de aard van de overeenkomst als de koop voorziet in levering van de digitale inhoud of digitale dienst."*.

In aanvulling hierop onderzoeken we (door toevoegen van FCIU-kenmerk 6: *"Gegarandeerde termijn voor beveiligingsupdates"*) of er een specifiekere of afwijkende termijn wordt gegeven voor 'beveiligingsupdates', omdat in dat geval relevant is om te onderzoeken hoe dit zich verhoudt tot de hierboven gegeven definitie.

De FCIU-kenmerken worden op drie momenten gemeten (dit wordt hieronder nader toegelicht bij de betreffende onderzoeksstappen):

- Precontractueel: de eigenschappen zijn opgezocht in de precontractuele informatie die is verzameld gedurende het selectie- en aankoopproces.
- Bij ingebruikname: verificatie van de *feitelijke* FCIU-eigenschappen.
- Na iedere update: controle van wijzigingen in feitelijke FCIU-eigenschappen.

3.2 Apparaatselectie

De volgende stap van de meting bestaat uit het samenstellen van de steekproefselectie van apparaten. In deze paragraaf lichten we toe hoe deze selectie tot stand komt.

3.2.1 Doelstelling en randvoorwaarden productselectieprocedure

Doel van dit onderzoek is, zoals eerder al aangegeven, zowel het ontwikkelen van een kader voor het uitvoeren van een meting, als het uitvoeren van de eerste meting. In dit document presenteren we een procedure voor het selecteren van een aantal domotica-

apparaten. Deze procedure leidt op navolgbare wijze tot een bruikbare selectie van apparaten ten behoeve van het uitvoeren van de beschreven meting.

Navolgbaarheid door het AT en de ACM is daarbij om twee redenen van groot belang:

1. **Herhaalbaarheid**. De meting dient door (of in opdracht van) het AT en de ACM in de toekomst te kunnen worden herhaald, waarbij de nieuwe resultaten moeten kunnen worden vergeleken met de in dit onderzoek verkregen resultaten.

2. **Bruikbaarheid van de resultaten**. Het is denkbaar dat het AT en/of de ACM vervolgacties verbinden aan concrete (apparaatspecifieke) uitkomsten van dit onderzoek. Het kan daarbij gaan om vervolgacties ten aanzien van een specifiek apparaat of een specifieke verkoper of fabrikant. Op basis van het *gelijkheidsbeginsel* zijn de beide toezichthouders gehouden gelijke gevallen gelijk te behandelen. Heel kort samengevat betekent dit dat het AT en de ACM objectief moeten kunnen rechtvaardigen dat in het geval van bepaalde specifieke apparaten, verkopers of fabrikanten handhavend wordt opgetreden, terwijl dit bij andere apparaten of partijen niet gebeurt.

Randvoorwaarden

Het selectiekader voor apparaten is ontworpen om te voldoen aan de volgende vereisten:

- **Compleet en deterministisch**. Het selectiekader moet geen ruimte laten voor keuzes die kunnen leiden tot andere uitkomsten wanneer de procedure op basis van dezelfde informatie opnieuw (bijvoorbeeld door een andere persoon of partij) zou worden uitgevoerd. Het opnieuw uitvoeren van de procedure op basis van de op het moment van de eerste uitvoering beschikbare informatie moet leiden tot dezelfde uitkomst als de eerste uitvoering. Een vereiste is uiteraard dat alle informatie wordt opgeslagen bij het uitvoeren van de procedure.

- **Representatief**. De procedure voor selectie van apparaten moet leiden tot een selectie die, rekening houdend met wat mogelijk is binnen de kaders van de onderzoeksopdracht, *representatief* is voor 'het aanbod van domotica-apparatuur gericht op de Nederlandse markt'.

- **Neutraal**. Gelijke apparaten moeten een gelijke kans hebben om te worden geselecteerd. Hiertoe definiëren we voor welke aspecten van een product een verschil wél mag leiden tot een verschil in selectiekans:
    - Technische (feitelijke) eigenschappen van het product (functionaliteiten, bouwkwaliteit, materialen);
    - Economische eigenschappen (prijs/prijssegment van het product);
    - Tijd die is verstreken sinds het product op de markt werd gebracht;
    - Marktaandeel van de producent of verkoper;
    - Verkrijgbaarheid van een product via verschillende kanalen (online, offline).

- De selectie is, voor wat betreft technische eigenschappen van de apparaten, **zo gevarieerd als mogelijk binnen de gestelde kaders**. De reden hiervoor is dat de meting in dit onderzoek (ook) bedoeld is om inzicht te krijgen in hoe het huidige aanbod van domotica-apparaten (de populatie) zich verhoudt tot de in de onderzoeksvraag benoemde regelgeving. Dit vraagt dat de steekproef generaliseerbaar is naar de populatie. Harde (statistische) generaliseerbaarheid is gezien de omvang van de steekproef in dit onderzoek niet mogelijk. Een grotere variatie van (technische eigenschappen van) apparaten binnen de steekproef zorgt er echter wel voor dat het

aantal verschillende onderdelen (denk aan besturingssystemen, softwarebibliotheken, et cetera) dat wordt geanalyseerd groter is. De kans is daardoor ook groter dat twee apparaten in de steekproef onderdelen gemeenschappelijk hebben.

Rationale

Alle 'slimme' apparaten zijn gebaseerd op een verzameling van technologieën om softwareapplicaties te bouwen en uit te voeren. Deze verzameling bestaat onder andere uit chipsets, besturingssystemen, softwarebibliotheken en (in sommige gevallen) white label-oplossingen.

Een voorbeeld is de ESP8266-chip, die kan en wordt toegepast in verschillende soorten slimme apparaten. Al deze apparaten maken gebruik van softwarebibliotheken die worden meegeleverd in de ESP8266-ontwikkelomgeving en de bijbehorende Wi-Fi-implementatie, en kunnen dan ook gedeelde zwakheden kennen. Door apparaten te selecteren die verschillende onderdelen gebruiken, minimaliseren we de kans dat dezelfde kwetsbaarheden meerdere keren worden gevonden binnen de steekproef (één keer constateren is voldoende als bekend is dat hetzelfde component ook in andere apparaten wordt gebruikt en 'bereikbaar' is). Daarmee maximaliseren we de 'virtuele scope' van het onderzoek (vinden we immers een zwakheid in de ESP8266-software, dan generaliseert dit mogelijk naar *alle* apparaten op de markt met deze chip en versie van de ontwikkelomgeving).

Scope

Vanuit de opdracht(gever) gelden de volgende eisen ten aanzien van de te selecteren apparaten:

- Het onderzoek richt zich op de domotica-apparaten die **door de consument verkrijgbaar zijn via de reguliere verkoopkanalen.**
    - Reguliere verkoopkanalen: zowel fysieke verkooppunten als online verkoopkanalen (een webwinkel, verkoopplatform of een combinatie daarvan).

- Het moet gaan om **verkoopkanalen via welke verkopers zich richten op de Nederlandse consument**. Dat betekent dat het gaat om fysieke winkels in Nederland. Als zij wijdverbreid zijn in Nederland hebben zij een potentieel breed bereik binnen Nederland. Bij online verkoop kan dit blijken uit een .nl domein (niet vereist), en/of het gebruik van de Nederlandse taal en levering in Nederland.

Voorgaande onderzoeken

Voor zover ons bekend zijn er geen vergelijkbare onderzoeken uitgevoerd in Nederland waarin een productselectieprocedure is gedefinieerd. In 2019 heeft Strict, in opdracht van AT, onderzoek gedaan naar de veiligheid van IoT- consumentenapparaten. [5] In dit rapport wordt echter niet toegelicht hoe tot de productselectie is gekomen. Hoewel de ACM intern diverse methoden en werkwijzen heeft ontwikkeld, is het nadrukkelijke verzoek vanuit de opdrachtgever aan de onderzoekers geweest om vanuit eigen perspectief een procedure te ontwerpen.

3.2.2 Vaststellen productcategorieën

De afgelopen jaren worden steeds meer apparaten 'slim' of 'smart' genoemd. Een formele definitie hiervan is niet te geven. Vaak wil het echter zeggen dat het apparaat kan worden gekoppeld aan een applicatie op een smartphone ('app') en/of een via internet aangeboden

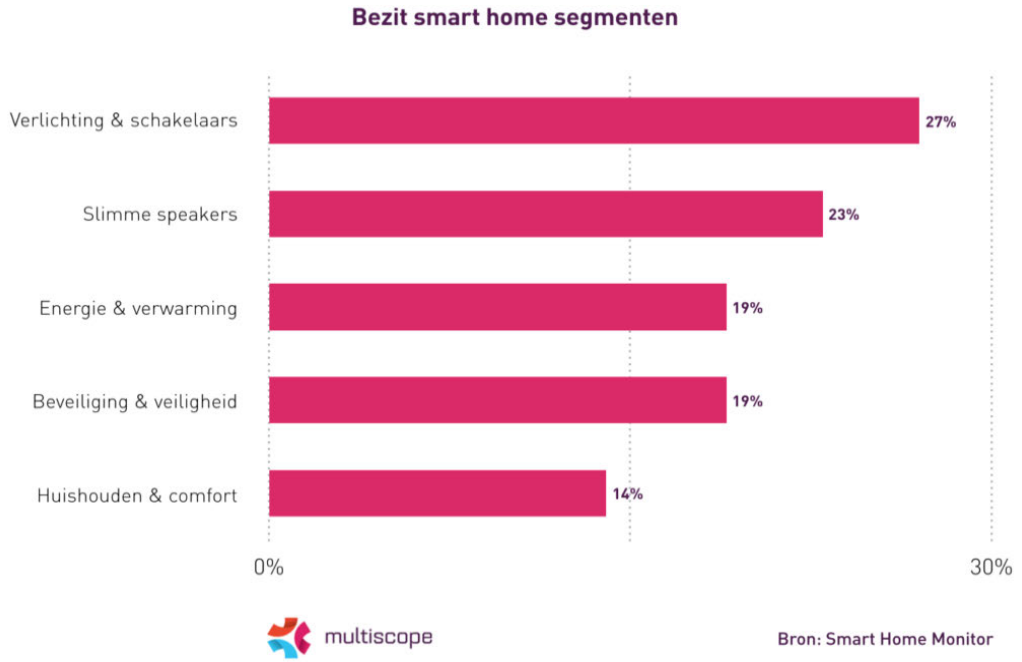
dienst. [6] In de categorie domotica betreft het slimme huishoudelijke apparaten. Sommige van deze apparaten kunnen met verschillende apps functioneren, terwijl voor andere één specifieke app noodzakelijk is (doorgaans van dezelfde fabrikant). In alle gevallen geldt echter dat het koppelen aan een app of dienst noodzakelijk is voor het apparaat om zijn functies te vervullen, dit maakt het een zaak met digitale elementen (zie par. 2.1)

Dit onderzoek omvat een deel van de apparaattypen binnen de categorie domotica. De opdrachtgever heeft in de onderzoeksopdracht de volgende categorieën gevraagd te bekijken:

- Domotica-hub met gekoppeld domotica-apparaat (zoals slimme lamp, gordijn, et cetera);
- Slimme babyfoon;
- Slimme televisie;
- Slim witgoed;
- Een nader te kiezen vijfde categorie.

We vullen de laatste categorie nader in door te kijken naar informatie over het verkoopvolume en bezit van domotica-apparaten op de Nederlandse markt en indelingen die daarbij gebruikt worden.

Domotica is redelijk eenvoudig onder te verdelen in categorieën: 'slimme' apparaten vallen vaak in categorieën elektronica die ook al voor 'niet-slimme'-apparaten bestonden (bijvoorbeeld: wasmachines, koelkasten, stofzuigers en babyfoons). Die indeling zien we dan ook het meest bij diverse grote webshops, zoals Bol.com, Coolblue en Mediamarkt, en op prijsvergelijkingswebsites zoals Kieskeurig en de Tweakers Pricewatch. De voorgestelde categorieën zijn daarin goed herkenbaar.



Figuur 1 Bezit smart home-apparaten voor Nederlandse huishoudens in 2021 (bron: [7])

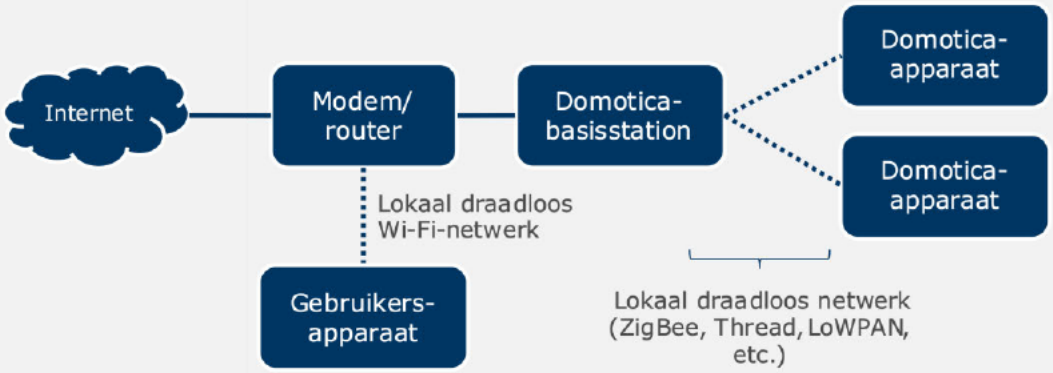
Marktonderzoeksbureau Multiscope hanteert een indeling op een iets hoger niveau in vijf categorieën. [8] Hierbij valt op dat slimme verlichting veruit de populairste vorm van

domotica is die op dit moment wordt gebruikt door Nederlandse consumenten. Het ligt dan ook voor de hand om de eerste categorie (domotica-hub met apparaat) te verbijzonderen naar 'domotica-hub met gekoppelde slimme lamp'. We verwachten overigens dat het vanuit oogpunt van digitale veiligheid relatief weinig uitmaakt wélk type apparaat er aan een domotica-hub gekoppeld is. Veelal gaat het namelijk om oplossingen waarbij veel logica in de app en hub is verwerkt en minder in het slimme apparaat (dat daardoor mogelijk ook goedkoper te produceren is en minder energie verbruikt). Vanuit oogpunt van functionaliteit, compatibiliteit en interoperabiliteit zijn daarnaast naar verwachting de hub en de app, en niet zozeer het slimme apparaat zelf, de bepalende factor.

Domotica-basisstations ('hubs')

Veel domotica-oplossingen maken gebruik van basisstations (ook 'hubs' genoemd). De reden hiervoor is dat veel domotica-apparatuur op batterijen werkt, en toepassing van Wi-Fi (vanwege het stroomverbruik) voor deze apparaten zou leiden tot een korte batterijduur. Daarom wordt voor dit soort apparaten vaak gebruik gemaakt van radiotechnologieën met laag energieverbruik die specifiek zijn ontwikkeld voor lokale draadloze netwerken. Voorbeelden hiervan zijn ZigBee, Z-Wave en Bluetooth.

Figuur 2 hieronder toont schematisch de rol van het domotica-basisstation in de communicatie tussen het domotica-apparaat en het internet en het gebruikersapparaat. Het basisstation (dat op een Wi-Fi- of bedraad netwerk kan zijn aangesloten) vormt als het ware een 'brug', waarover (via een onlinedienst of op basis van lokale communicatie) kan worden gecommuniceerd met de verbonden domotica-apparaten.

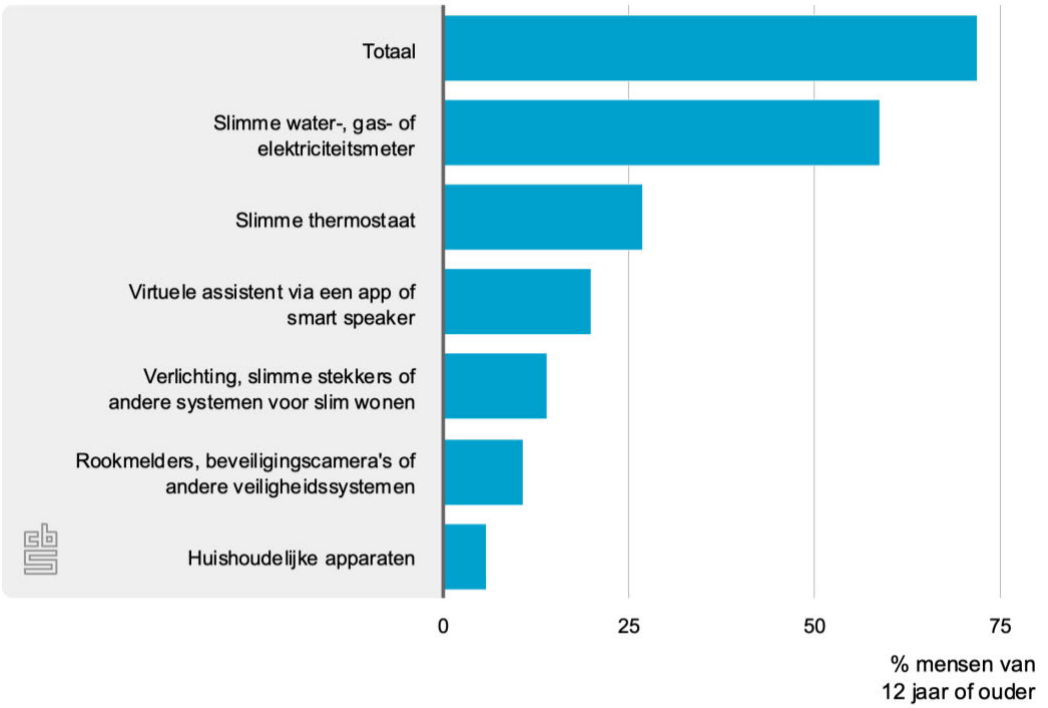


Figuur 2 Schematische weergave van de rol van een domotica-basisstation in de communicatie tussen een domotica-apparaat, het internet en het gebruikersapparaat, in een gangbaar scenario voor consumenten thuis.

In dit onderzoek beschouwen we de combinatie van hub en aangesloten apparaat als één geheel bij het analyseren van de technische eigenschappen zoals de digitale veiligheid. Sommige apparaten kunnen zowel met als zonder hub (bijvoorbeeld via Bluetooth) werken. In dat geval nemen we de hub desondanks mee.

Op het eerste gezicht lijkt er verder weinig overlap tussen de geselecteerde categorieën en de indeling van Multiscope. Merk hierbij echter op dat de slimme babyfoon valt onder "beveiliging en veiligheid" en slim witgoed (wasmachines, drogers, vaatwassers) onder "huishouden en comfort". De slimme televisie is niet meegenomen door Multiscope, maar dit lijkt desondanks een (in verkoopvolume) belangrijke categorie te zijn (zie o.a. [9]). Afgaand op deze categorieën lijkt een zinvolle toevoeging aan de selectie

productcategorieën een categorie binnen "energie en verwarming", waarbij de slimme thermostaat het meest voor de hand ligt: het CBS rapporteert dat in 2020 naar schatting 27% van de mensen van 12 jaar of ouder aangaf een slimme thermostaat te hebben. (Figuur 3 en [10]).



Figuur 3 Bezit van slimme apparaten door Nederlanders van 12 jaar of ouder in 2020 (bron: [10])

Zowel CBS, Multiscope als andere bronnen merken de slimme speaker als populair. Deze categorie heeft enige overlap met de categorie "domotica-hub" omdat het hier gaat om apparaten waarmee (via een 'digitale assistent') ook andere apparaten kunnen worden aangestuurd.

De categorie 'slim witgoed' tot slot lijkt van deze categorieën de minst ontwikkelde. Voorbeelden van producten die onder deze categorie vallen zijn slimme koelkasten, wasmachines, vaatwassers en ovens. De slimme koelkast sluit daarmee wellicht het beste aan op de toekomstvisie van een 'slim huishouden': al in de jaren '80 en '90 werd een slimme koelkast, die automatisch nieuwe producten bestelt als de voorraad op raakt, getoond in het 'Huis van de Toekomst'. [11] Toch lijkt deze categorie zich langzamer te ontwikkelen dan de andere. Vanwege het beperkte aanbod aan slimme koelkasten in Nederland en de relatief hoge prijs[54] is ervoor gekozen deze productcategorie daarom buiten beschouwing te laten. In plaats daarvan achten wij de slimme wasmachine als een veel voorkomend en goedkoper product binnen de categorie slim witgoed.[55] Uit cijfers van marktonderzoeksbureau GfK blijkt namelijk dat ruim een kwart (26%) van de verkochte

[54] Voor de Samsung Family Hub (614L) RS6HA8891SL geldt bijvoorbeeld een prijs van € 2.089,- (d.d. 4 augustus 2022) en voor de Family Hub (614L) RS6HA8891B1 geldt een prijs van € 2.299,- (d.d. 4 augustus 2022), via de website van Samsung. Deze koelkasten bestellen niet automatisch producten als de voorraad op raakt.

[55] De slimme koelkast in deze zin van het woord wordt in veel literatuur aangehaald, maar lijkt in populariteit ingehaald door andere slimme apparaten, waaronder ander slim witgoed.

wasmachines in Nederland smart is. [12] We verbijzonderen de categorie slim witgoed daarom naar "slimme wasmachine".

Onderstaande Tabel 2 toont de uiteindelijke selectie productcategorieën.

Tabel 2 Overzicht van in het onderzoek gehanteerde productcategorieën

Volgorde	Categorie	Zoekterm	Aantal apparaten
1	Domotica-hub met gekoppelde slimme lamp[56]	"slimme verlichting"	3
2	Slimme babyfoon	"slimme babyfoon"	3
3	Slimme televisie	"smart tv"	3
4	Slimme thermostaat	"slimme thermostaat"	3
5	Slim witgoed	"slimme wasmachine"	3

De productselectieprocedure (hieronder) wordt sequentieel toegepast op iedere productcategorie. De volgorde waarin dit gebeurt is gebaseerd de in Tabel 2 aangegeven volgorde van productcategorieën. Deze is alfabetisch op de categorienaam zoals getoond in de tabel.

Per categorie selecteren we drie apparaten. Dit aantal komt voort uit de wens van de opdrachtgever om minimaal 15 apparaten te onderzoeken, en het budget dat voor dit onderzoek beschikbaar is voor de aanschaf van de apparaten. Van de drie apparaten per categorie kopen we er steeds twee online en één bij een 'offline' (fysieke) winkel.

In vervolgonderzoeken kunnen deze categorieën uiteraard anders worden gedefinieerd – de argumenten die spelen bij dit onderzoek zijn niet noodzakelijkerwijs dezelfde als voor toekomstig toezicht.

3.2.3 Selectieprocedure per categorie

Figuur 4 hieronder toont een schematische weergave van de stappen waarmee per categorie een set apparaten wordt geselecteerd voor de steekproef. Hieronder worden elk van de vijf stappen in meer detail toegelicht.

[56] In deze categorie wordt de eerste slimme lamp gekocht die in combinatie met een bijbehorend basisstation (hub) wordt aangeboden. Over het algemeen gaat het hierbij om een 'starterkit'. Wanneer er geen hub wordt aangeboden in combinatie met een slimme lamp, wordt binnen de categoriepagina van diezelfde winkel gezocht op "slimme verlichting starterkit". Wanneer in de zoekresultaten geen hub wordt geretourneerd wordt de winkel als geheel overgeslagen.

Figuur 4 Schematische weergave productselectiekader

Stap 1. De onderzoeker zoekt met de zoekmachine die het meest wordt gebruikt in Nederland op de productcategorie als zoekterm ("slimme babyfoon").

Daarbij gebruiken we de Nederlandstalige versie van de zoekmachine (in geval van de nulmeting is dit Google Chrome[57]), vanaf een IP-adres dat hoort bij een Nederlandse consumenten-ISP, en zonder te zijn ingelogd. We nemen diverse maatregelen om te voorkomen dat getoonde zoekresultaten gebaseerd zijn op eerder persoonlijke zoekgedrag (zie de toelichting hieronder onder 'Rationale').

De zoekterm plaatsen we (indien de zoekmachine dit ondersteunt) tussen dubbele aanhalingstekens, als deze uit meerdere woorden bestaat. Zo voorkomen we dat resultaten alleen relateren aan één van de woorden.

Rationale

Het oriëntatie- en aanschafproces van een consument kan er op veel verschillende manieren uitzien. Het voert te ver om ál deze paden na te bootsen. Voor het maken van een adequate productselectie is het volgen van een veelvoorkomend pad toereikend.

We veronderstellen dat een groot deel van de consumenten in het aankoopproces gebruik maakt van een zoekmachine om een product en aanbieder daarvan te vinden. [13]

We kiezen ervoor om een oriëntatie- en aankoopproces te simuleren dat zich grotendeels online afspeelt (de offline aankopen zijn dus het gevolg van een online oriëntatieproces waarin ook een fysieke winkel wordt gezocht). Gezien de productcategorie (domotica) lijkt dit ons het meest aannemelijke en ook een representatief scenario. Multiscope concludeert in oktober 2021 dat de meeste aankopen van slimme producten bij Bol.com worden gedaan. Daarnaast associëren de meeste Nederlanders de Mediamarkt (22%) en Coolblue (22%) met domotica. [14]

De zoekresultaten van moderne zoekmachines zijn sterk afhankelijk van wat de zoekmachine weet over de gebruiker. Vaak kan uit allerlei kenmerken van de browser en

[57] De keuze voor Google Chrome is gebaseerd op het feit dat dit eind 2021 de meest gebruikte browser is in Nederland. [27] [28]

de internetaansluiting worden afgeleid in welk land een gebruiker zich bevindt, welke taal deze spreekt, et cetera. Deze informatie wordt gebruikt om relevantere zoekresultaten (bijvoorbeeld gericht op het eigen land of de taal) hoger te tonen. Via cookies en tracking kunnen zoekmachines eventueel meer informatie onthouden en meenemen. Hiermee dient dan ook rekening te worden gehouden bij het uitvoeren van de zoekopdrachten. In de nulmeting doen we dit door de volgende maatregelen te treffen:

- We gebruiken een 'schone' computer (een werklaptop van Dialogic met een 'leeg' gebruikersprofiel). De taalinstelling is Nederlands.
- We gebruiken een consumenteninternetverbinding (dus niet die van het kantoor van Dialogic). Hierbij gaat de voorkeur uit naar een aansluiting waarbij IP-adressen worden gedeeld tussen verschillende abonnees, waardoor identificatie op basis van het publieke IP-adres moeilijker is. [15]
- We gebruiken de incognitomodus van de browser, die ervoor zorgt dat deze de bezoekgeschiedenis, cookies en sitegegevens niet opslaat. Daardoor minimaliseren we 'volgorde-effecten' (cookies geplaatst in een eerdere stap van deze procedure zouden volgende stappen kunnen beïnvloeden).[58] Dergelijke effecten zijn echter niet volledig uitgesloten.

Bedrijven kunnen advertenties plaatsen die verschijnen tussen de zoekresultaten. Deze advertenties worden niet meegenomen, omdat de volgorde van tonen sterk afhankelijk is van diverse factoren, waaronder hoeveel de plaatser van de advertentie betaalt. De niet-advertentieresultaten zijn dan ook het meest bruikbaar in het kader van dit onderzoek.

Stap 2. De onderzoeker noteert, op volgorde van de zoekresultaten, drie kanalen.

De drie kanalen worden genoteerd in onderstaande volgorde en zijn:

a. **De eerste twee online webwinkels** waarbij ten minste één product wordt verkocht binnen de categorie, met indicatie levertijd binnen vijf werkdagen.

---

[58] De *incognitomodus* van Chrome voorkomt dat de bezoekgeschiedenis en de gegevens die gedurende de incognitosessie door websites worden opgeslagen op de computer van de gebruiker (zoals cookies) permanent worden opgeslagen. Bij het sluiten van de incognitomodus verwijdert de browser deze gegevens. Daarnaast zijn gegevens die eerder buiten de incognitomodus zijn opgeslagen, niet benaderbaar vanuit de incognitomodus. De incognitomodus zorgt er zo voor dat een website op basis van technieken als cookies een individuele gebruiker niet meer eenvoudig kan identificeren, tenzij deze binnen de incognitosessie is geïdentificeerd. [30] De incognitomodus voorkomt echter niet de identificatie op basis van technieken als 'fingerprinting' (identificatie op basis van unieke eigenschappen van de browser en/of computer van de gebruiker) en bijvoorbeeld op basis van het publieke IP-adres (dat immers niet wijzigt bij inschakelen van de incognitomodus). Daarnaast kan de gebruiker gedurende een incognitosessie gevolgd worden op basis van cookies die zijn opgeslagen gedurende deze sessie. Het is daarom van belang de incognitosessie steeds opnieuw te starten tussen de aankopen. Een andere manier om hetzelfde effect te bereiken is het steeds gebruiken van een nieuw gebruikersprofiel in de browser. Om de mogelijkheden tot fingerprinting te minimaliseren kan aanvullend gebruik worden gemaakt van een 'geschoond' gebruikersprofiel in het besturingssysteem of zelfs een volledig geschoond systeem. Om identificatie op basis van het IP-adres te voorkomen kan aanvullend gebruik worden gemaakt van een VPN-verbinding of een internetaansluiting waarbij gebruikers hetzelfde publieke IP-adres delen (zie voor toelichting [15]). Overigens kan het gebruik van een VPN-verbinding mogelijk worden gedetecteerd door een website, omdat het verkeer vanuit perspectief van de website dan niet vanuit het netwerk van een Nederlandse internetaanbieder afkomstig is.

In de gehele set van 15 apparaten mag maximaal drie keer dezelfde winkel voorkomen. Wanneer een bepaalde winkel al drie keer voorkomt (in totaal, dus ook als de winkel 2x als webshop en 1x als fysieke winkel voorkomt), slaan we deze bij de volgende productcategorieën over.

Daarnaast dient de webwinkel gericht te zijn op Nederlandse consumenten. Aan deze laatste eis wordt tegemoetgekomen wanneer aan de volgende criteria wordt voldaan:

i. De website is in het Nederlands, en/of heeft een .nl-domeinnaam;
ii. De website is een webshop waarop een consument een product uit de genoemde categorie kan bestellen (deze linkt hiervoor dus niet door naar een ándere webshop).[59]
iii. De webshop levert in Nederland en/of heeft een fysieke winkel in meerdere provincies in Nederland, waar kan worden afgehaald. Het is de winkel toegestaan specifieke gebieden uit te sluiten of andere leveringstermijnen te hanteren voor bepaalde gebieden in Nederland (denk aan de Waddeneilanden).

Het is dus niet vereist dat de betreffende webshop meerdere fysieke vestigingen heeft in Nederland (zolang deze in Nederland levert). De gevonden webwinkel kan ook een online shop van een fabrikant of importeur zijn (waar slechts één merk of zelfs één type apparaat wordt verkocht).

b. **De eerste winkel(keten) met meerdere vestigingen in Nederland** (in meerdere provincies) waarbij ten minste één product wordt verkocht binnen de categorie, en standaard op voorraad is bij ten minste één vestiging in de provincie Utrecht (om logistieke redenen). Daarnaast dient het product in de winkel aangeschaft te kunnen worden zonder het eerst online te reserveren (click-and-collect). Het maakt niet uit of de website daarnaast ook fungeert als webshop voor dezelfde keten. Wanneer de kandidaat ook al bij (a) zou worden geselecteerd binnen dezelfde categorie, selecteren we de volgende kandidaat. Als de kandidaat al het maximale aantal keer bij (a) is geselecteerd in het gehele onderzoek, selecteren we de volgende kandidaat.

   In het gehele onderzoek willen we iedere 'offline' winkelketen daarnaast slechts één keer laten voorkomen als 'offline' winkelketen. De reden hiervoor is dat het aantal offline-winkels beperkt is (zie hierboven). Binnen deze kleinere set levert een dubbeling dan ook substantieel minder variatie op.

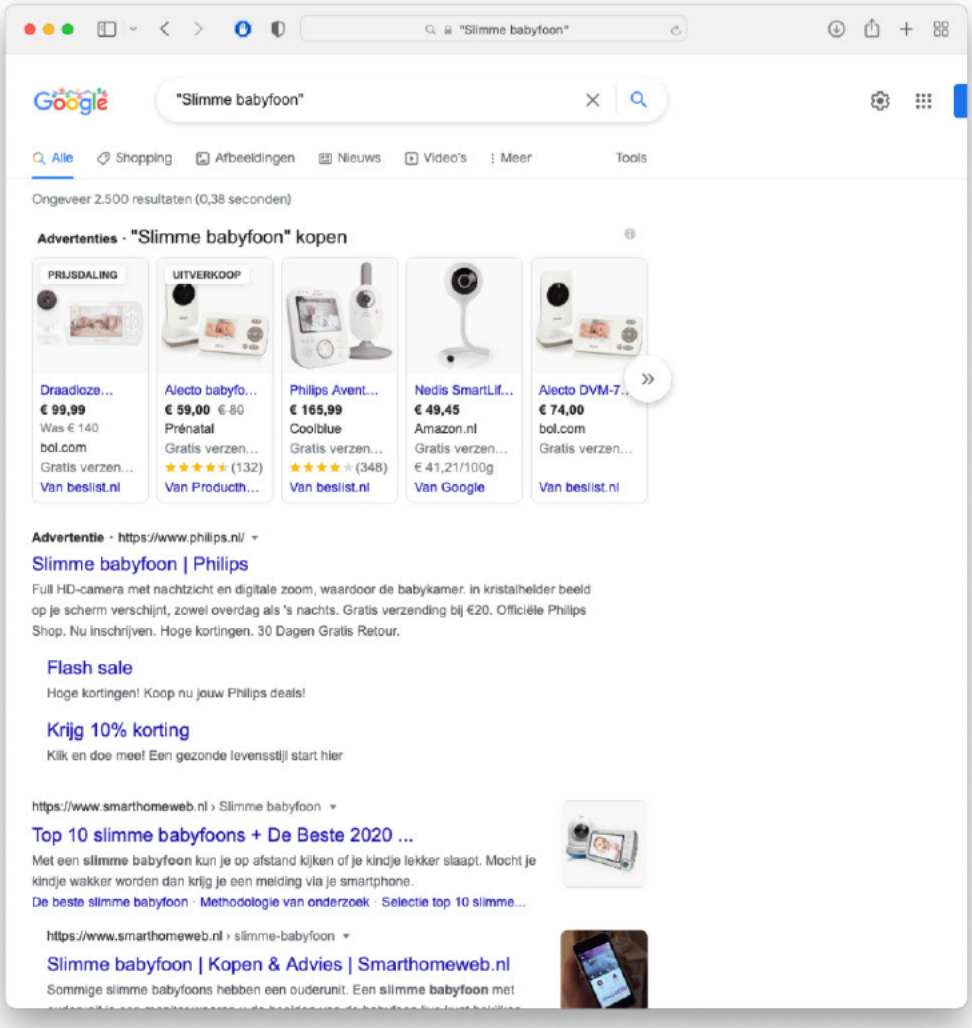
   Als een al geselecteerde offline-winkel opnieuw bovenaan staat, kiezen we de volgende (net zo lang tot een nog niet geselecteerde winkel is gevonden). In het uitzonderlijke geval dat er geen winkel is die voldoet kiezen we de eerste kandidaat, maar een andere vestiging van deze keten.

[59] Hieronder vallen dus niet prijsvergelijkingswebsites, maar wel 'marktplaatsen' / tussenhandeldiensten waarop meerdere verkopers hun waar aanbieden, maar waarbij de orderafhandeling geschiedt door de marktplaats (Bol.com Plaza, een deel van het aanbod van Amazon, e.a.).

Rationale

In het onderzoek meten we in hoeverre precontractuele informatie overeenstemt met de feitelijke situatie nadat de aankoop heeft plaatsgevonden. Verondersteld kan worden dat de wijze waarop precontractuele informatie beschikbaar is en wordt verstrekt bij online aankopen sterk afwijkt van 'offline' aankopen.

In de praktijk is overigens ook een combinatie van online- en offline-informatieverstrekking denkbaar. Een consument bezoekt doorgaans eerst de website van de winkel en gaat er dan naartoe, of bekijkt producten eerst in de winkel en koopt ze daarna online. [16] Juridisch kan de verkoper in een winkel er niet zomaar van uitgaan dat er online al informatie aan de consument verstrekt is. Daarnaast is het juridisch gezien de vraag of in een dergelijk scenario aan de vereisten voor het *moment* van informatieverstrekking wordt voldaan. [17]



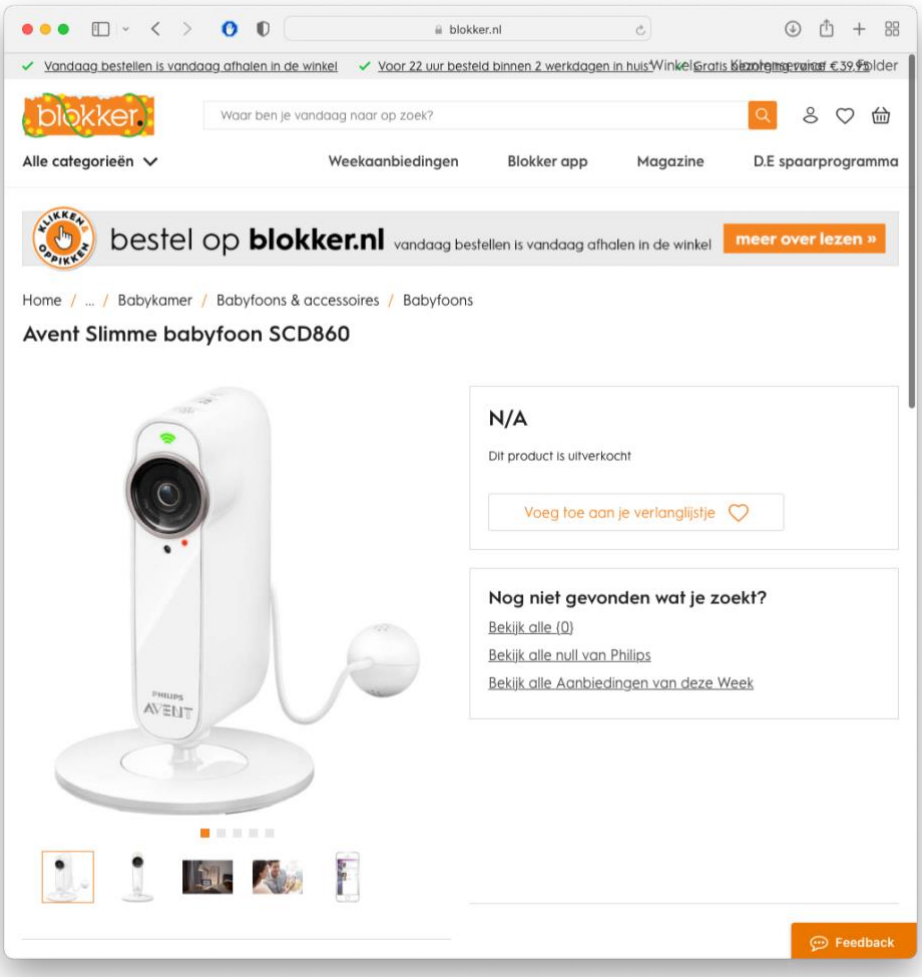
Figuur 5 Voorbeeld van het resultaat van de beschreven zoekactie. De resultaten met vermelding "Advertentie" worden genegeerd. Smarthomeweb.nl is in dit voorbeeld de eerste vergelijkingssite.

Advertenties en andere plaatsingen van zoekresultaten (gesponsorde content) worden in deze procedure genegeerd. De procedure kan voortgaan wanneer een resultaat voor ten minste één van de hierboven genoemde categorieën zijn gevonden.

Stap 3. Per kanaal openen we, op basis van de website, de eerst bovenliggende categoriepagina voor de gezochte categorie.

Een categoriepagina is een pagina waarop meerdere verschillende producttypen binnen de gezochte categorie worden getoond. Bij het openen van de categoriepagina worden alle cookies geaccepteerd en worden eventuele pop-ups (bijv. aanbiedingen) weggeklikt.

- In veel gevallen zal het zoekresultaat verwijzen naar een categoriepagina. Dit is in dat geval de gezochte pagina.
- Wanneer het zoekresultaat verwijst naar een pagina van een enkel product, klikt de onderzoeker door naar een categoriepagina waarop dit product wordt genoemd en waarvan de titel zo dicht mogelijk bij de gezochte categorie ligt.



Figuur 6 Voorbeeld van een productpagina bij een winkelketen met fysieke winkels en een webshop. De categoriepagina is te bereiken door linksboven op "Babyfoons" te klikken. Merk op dat deze ook niet-slimme babyfoons kan bevatten.

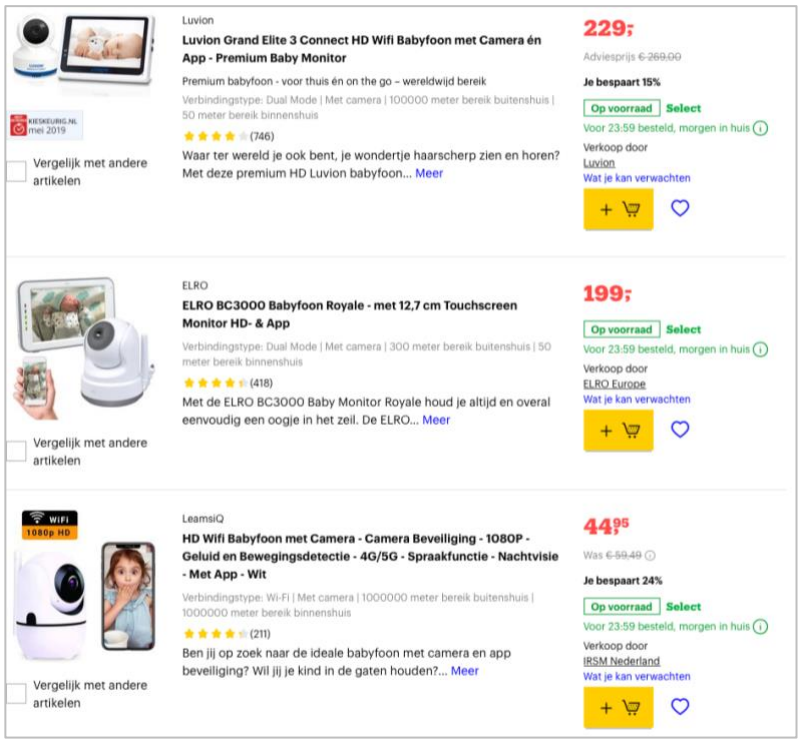
Rationale

Online en offline winkels hebben een sterke prikkel om op hun website een beeld van het assortiment te scheppen dat aantrekkelijk is voor zoveel mogelijk potentiële kopers. Door gebruik te maken van deze informatie (verbijzonderd naar de productcategorie, dus op categoriepagina's) ontstaat een steekproef die representatief is voor de set apparaten die het meest wordt verkocht.

Stap 4. Van de geopende categoriepagina's noteren we het populairste product, mits leverbaar

De categoriepagina wordt gesorteerd op basis van populariteit (o.a. populairst, meest verkocht[60]). Indien niet op populariteit kan worden geselecteerd, wordt de default sortering gebruikt. Een voorwaarde bij de gebruikte sortering is dat deze consequent hetzelfde productoverzicht dient te retourneren. Wanneer niet aan deze voorwaarde wordt voldaan, slaan we de winkel als geheel over. In beginsel noteren we het bovenste product om via dit kanaal aan te schaffen. Advertenties van producten of anderszins geplaatste vermeldingen (gesponsorde content) worden niet genoteerd. Een product wordt ook niet genoteerd wanneer de levertijd meer dan 5 werkdagen bedraagt. De reden hiervoor is tweezijdig: 1) In verband met de planning van het onderzoek is het praktisch om de apparaten zo snel mogelijk geleverd te krijgen en 2) Het is waarschijnlijk dat een consument ook een dergelijke overweging maakt wanneer hij een product online bestelt. In het kader van administratie worden de eerste tien gepresenteerde apparaten, die aan bovenstaande eisen voldoen, opgeslagen.

[60] De invulling van dit begrip wordt bepaald door de winkel en kan ook gebaseerd zijn op bijvoorbeeld het aantal keer dat een product is bekeken.



Figuur 7 Voorbeeld van een categoriepagina van een webshop (hier bol.com). Merk op dat de apparaten die worden verkocht worden geleverd door verschillende partijen, maar dat het bestelproces verloopt via deze website.

Stap 5. We controleren het apparaat op prijs en dubbeling

Voordat het apparaat wordt aangeschaft vinden nog enkele checks plaats.

Apparaten die met een significant hogere prijs dan gemiddeld worden aangeboden (meer dan 15% boven de mediaanprijs[61] die voor het product in een prijsvergelijker wordt gegeven) worden overgeslagen. Daarnaast wordt een bovengrens voor de prijs gehanteerd van € 1.000,- (inclusief Btw) per apparaat. Apparaten met een prijs boven deze bovengrens worden overgeslagen.

Vervolgens wordt gecontroleerd of er niet al een vrijwel identiek product is geselecteerd om aan te schaffen (bij een andere winkel). Indien dit wel het geval is, wordt in stap 4 het volgende product gekozen. Een product is 'vrijwel identiek' indien aan een van de volgende criteria wordt voldaan:

- Het is een product van dezelfde fabrikant. Hiermee wordt de diversiteit zo groot mogelijk gehouden. Bijvoorbeeld:
    a. Het is exact hetzelfde product of verschilt enkel in kleur/taal/verpakking/uitvoering.
    b. Het is een andere versie in dezelfde productserie ("[redacted] v1", "[redacted] v2")
- Een van de twee apparaten is een combinatiebundel ("3-in-1" pakketten of "startersbundels") en het andere product is een los product uit die bundel.

[61] De *mediaanprijs* verdeelt een reeks verkopen in twee gelijke delen. Indien de mediaanprijs bijvoorbeeld 500 euro bedraagt, dan lag de prijs bij de helft van de verkopen onder 500 euro en bij de andere helft boven dat bedrag.

Rationale

Sommige fabrikanten brengen een groot aantal varianten van hetzelfde product op de markt, bijvoorbeeld met een handleiding in een andere taal, of in een andere kleur. Vanuit het perspectief van een belangrijk deel van de onderzoeksvragen zijn deze variaties niet zo interessant. Door deze varianten te 'ontdubbelen' komt plaats vrij in het onderzoek voor andere apparaten.

In het geval dat een geselecteerd product niet binnen de vastgestelde termijn van 5 werkdagen wordt bezorgd, wordt het product geselecteerd dat oorspronkelijk na dit product in de categorielijst van dezelfde winkel was opgenomen (stap 4).

3.3 Verzamelen van precontractueel verstrekte informatie en aankoop

Gedurende en na de aankoop van de apparaten in de steekproef verzamelen we productinformatie van de verkoper en fabrikant. Centraal daarin staat de vraag of een gemiddelde consument[62] weet (of kan weten) wat hij koopt, en of het beloofde, ook na verloop van tijd, wordt waargemaakt of verandert. We kijken hierbij naar de informatie die wordt verstrekt over de eerder geselecteerde FCIU-kenmerken (Tabel 1).

3.3.1 Randvoorwaarden

De informatieverzameling is ingevuld op basis van een aantal randvoorwaarden. Een randvoorwaarde van de opdrachtgever is dat de oorspronkelijke informatieverstrekking vastgelegd dient te worden op dusdanige wijze dat de oorspronkelijke uiting in zijn context beoordeeld kan worden en de datum en het tijdstip van de uiting buiten twijfel verheven zijn. Dat betekent onder meer dat het formaat waarin de uiting is beoordeeld duidelijk moet zijn: het moet duidelijk zijn op welk apparaat met welke instellingen de uiting is vastgelegd. Bij bijvoorbeeld informatie in de fysieke winkel betekent dit dat bijvoorbeeld de plaats en de omvang van het informatiebord duidelijk moeten zijn.

Hieronder werken we uit hoe we de benodigde informatie verzamelen en hoe wordt voldaan aan deze randvoorwaarden. We maken daarbij onderscheid tussen online en offline aankopen, omdat de wijze waarop informatie wordt verstrekt in beide gevallen uiteraard sterk verschilt.

3.3.2 Online informatieverzameling

Omdat de informatie die voor en tijdens de aankoop wordt verstrekt na verloop van tijd kan wijzigen (of zelfs niet meer beschikbaar kan raken) is het belangrijk dat alle benodigde informatie achtereenvolgens wordt verzameld. Het startpunt hiervoor is de eerste productpagina van de verkopende webwinkel en alle vervolgpagina's die een bezoeker tegenkomt bij het voltooien van het aankoopproces. Op deze pagina zijn typisch allerlei kenmerken van het product te vinden, waaronder technische specificaties rondom FCI.

Gerichte informatieverzameling binnen door verkoper verstrekte informatie

De werkwijze is als volgt: we bekijken de productpagina en gaan specifiek op zoek naar de informatie op de hierboven genoemde aspecten. De informatie noteren we in een separaat document. Tijdens de informatieverzameling wordt het beeldscherm opgenomen (als video

[62] Zie juridisch kader voor de definitie hiervan.

en als volledige schermafbeelding van iedere pagina, ook wanneer een pagina 'wijzigt' doordat er een pop-up wordt geopend). Hierdoor is achteraf te achterhalen op welke locatie bepaalde informatie voorkwam (in sommige gevallen is informatie namelijk pas zichtbaar zodra er wordt geklikt op een link, waarna een 'pop-up' binnen de pagina opent).

Tijdens het aankoopproces mag ten behoeve van de informatieverzameling worden geklikt op alle links en knoppen die een webwinkel op de betreffende pagina's aanbiedt. Wij openen alle links die enigszins relevant lijken. De beoordeling of dat past bij het gedrag van een 'gemiddelde consument' valt buiten de scope van het onderzoek, maar kan uiteraard achteraf worden gemaakt.

Alle verzamelde gegevens worden voorzien van datum en tijd en samengevoegd in een archief. Zodra het aankoopproces is afgerond sluiten we het archief af. Eventuele nagekomen informatie van de verkoper (denk aan e-mails van de webwinkel) worden opgeslagen in een nieuw archief, dat we wekelijks afsluiten.

Ongerichte informatieverzameling: bredere opname van door verkoper verstrekte informatie

Een aandachtspunt is dat deze informatie niet altijd precies of eenduidig is geformuleerd. Zo zijn we in het vooronderzoek productpagina's tegengekomen waar simpelweg staat "werkt met een smartphone", terwijl het voor het beoordelen van FCI relevant is om te weten op/met welke smartphones (platform en versie) het product werkt. Soms is deze informatie te vinden op subpagina's (een voorbeeld is de pagina "Dit product werkt met de volgende apparaten" bij een van de webshops die we bekeken). We willen de mogelijkheid openlaten om bij het maken van de vergelijking achteraf de beschikking te hebben over een bredere set van informatie.

Om bovengenoemde redenen kiezen we ervoor om naast het verzamelen van specifieke informatie van de productpagina en verdere pagina's in het bestelproces ook (geautomatiseerd) diverse subpagina's te verzamelen. We doen dit door alle links (tot drie niveaus diep) vanaf de productpagina te volgen en deze pagina's op te slaan. Op het eerste niveau volgen we daarbij ook links die buiten de website van de winkel verwijzen (zodat bijvoorbeeld links naar een handleiding of productconformiteitsverklaring wordt meegenomen), op de diepere niveaus doen we dit niet.

De bredere informatieverzameling leidt tot een archief van zowel schermafbeeldingen (van hele pagina's) als kopieën van de webpagina zelf (als HTML-archief), inclusief eventuele bijlagen (zoals PDF-bestanden).

Gerichte informatieverzameling website producent

Via een link op de productpagina van de webwinkel proberen we de juiste pagina's bij de producent te vinden. Als de webwinkel niet verwijst naar de producent voeren we een zoekactie uit via een zoekmachine en bezoeken we de eerste 'hit' op de website van de fabrikant die over het specifieke product gaat (zie daarbij de opmerkingen rondom het gebruik van zoekmachines in het hoofdstuk over de productselectiemethode).

Vanaf de productpagina van de producent wordt op hoofdlijnen dezelfde informatie verzameld (en op dezelfde wijze) als hierboven beschreven. Concreet zoeken we aanvullend naar de volgende elementen:

- "End User License Agreements" (EULAs) die een gebruiker zou moeten accepteren bij ingebruikname van het product (de vraag hierbij is of deze pas op moment van ingebruikname van het product worden getoond, of dat ze vooraf in te zien zijn via de producent).

- "Terms of service" die van toepassing zijn op de app(s) van de fabrikant die nodig zijn om het product te gebruiken.
- Conformiteitsverklaringen ten aanzien van regelgeving, zoals de Radiorichtlijn.

Verkoopvoorwaarden van de fabrikant (indien deze ook producten verkoopt) worden niet meegenomen. Deze zijn alleen relevant als het product daadwerkelijk bij de fabrikant wordt gekocht.

Ongerichte informatieverzameling website producent

In aanvulling op bovenstaande wordt ook ongericht informatie verzameld, analoog aan de hierboven beschreven procedure.

3.3.3 Offline informatieverzameling

Voor de offline aankopen wordt alle informatie meegenomen die in of in de directe omgeving van de winkel wordt verstrekt, zoals bijvoorbeeld op borden en posters. De informatieverzameling gebeurt altijd door een team van twee onderzoekers en bestaat uit een gesprek met een medewerker, waaraan enkele vragen worden gesteld, en het maken van foto's van relevante borden, posters of andere informatiedragers. Er worden geen gesprekken opgenomen. Direct na het verlaten van de winkel worden aantekeningen gemaakt van het gesprek met de medewerker en eventuele andere relevante details.

Mocht de onderzoekers worden gevraagd of zij bezig zijn met een onderzoek, of mystery shoppers zijn, zullen zij hier open over zijn. Het is echter in het belang van het onderzoek om behandeld te worden als een gewone consument. Om de kans te minimaliseren dat het gesprek met de medewerker anders verloopt vanwege vermoedens van mystery shopping, zullen de foto's van alle informatie pas worden gemaakt nadat het gesprek met de medewerker is afgerond. Algemeen uitgangspunt is dat de onderzoekers zich zo veel mogelijk gedragen als normale consumenten.

Voorbereiding

De onderzoekers bezoeken de winkel met twee personen. Zij weten welk product ze willen kopen en welke vragen zij gaan stellen. Zij hebben hun smartphone bij zich om foto's te maken en middelen om direct na de aankoop aantekeningen van het gesprek te maken.

Informatieverzameling – gesprek

Onderzoekers zoeken het product in de winkel en spreken een medewerker aan om enkele vragen te stellen.

Functionaliteit, compatibiliteit en interoperabiliteit

De vragen over deze onderwerpen zullen na de selectie per apparaat worden bepaald, voorafgaand aan het winkelbezoek. Het zal namelijk per apparaat verschillen wat op dit gebied logische vragen zijn om te stellen. In ieder geval zullen per apparaat vragen worden gesteld over alle drie deze onderwerpen. Voorbeelden van vragen zijn:

1. Wat kan deze wasmachine vergeleken met een 'domme' wasmachine?
2. Kan ik hem ook bedienen met een Android-telefoon?
3. Krijg ik een seintje op mijn telefoon wanneer mijn was klaar is?

Hoewel vooraf wordt bepaald welke vragen de onderzoekers in principe zullen stellen, kan het zijn dat bepaalde vragen niet meer logisch zijn om te stellen vanwege het antwoord op een vorige vraag. Ook kan een onvoorziene vraag juist heel erg voor de hand liggen naar aanleiding van een bepaald antwoord. De onderzoekers zullen zich gedragen als een consument die de zaak binnenkomt met, bijvoorbeeld, bovenstaande drie vragen. Zij zullen

daarom de logische vragen stellen tot aan de informatiebehoefte van een normale consument voldaan zou zijn.[63]

Updatebeleid

Voor elk aan te schaffen product zal worden gevraagd naar het updatebeleid. Dit gebeurt in beginsel met de open vraag 'hoe zit het met updates?' Afhankelijk van het antwoord vragen we door over hoe lang en hoe vaak updates zullen worden ontvangen.

Informatieverzameling – foto's

Het is goed denkbaar dat in en rondom de winkel borden staan of posters hangen met informatie die betrekking heeft op het aan te schaffen product. Hiervan worden foto's gemaakt. Zoals eerder genoemd gebeurt dit in principe pas nadat het gesprek met de medewerker is afgerond.[64]

Verslaglegging

Direct na de aankoop bespreken de onderzoekers het proces en de verkregen informatie, waarbij zij aantekeningen maken. Deze aantekening worden vervolgens uitgewerkt in een verslag per aankoop, waarin de mondeling verkregen informatie en de genomen foto's worden ingevoerd. Uiteraard worden hier ook metadata, zoals datum, tijd en winkel, in opgenomen.

3.3.4 Analyse van de verzamelde informatie

Op basis van de verzamelde informatie worden de volgende vergelijkingen gemaakt (Tabel 3).

Tabel 3 Overzicht van de vergelijkingen die worden gedaan tussen verzamelde informatie

Moment vergelijking	Welke informatie	Met welke andere informatie
Kort na aankoop	De informatie die de verkoper voor/tijdens de aankoop verstrekte	De informatie die de fabrikant op moment van aankoop verstrekte
Kort na de aankoop en ingebruikname	Staat van het product bij ingebruikname	De informatie die de verkoper voor/tijdens de aankoop verstrekte
Kort na de aankoop en ingebruikname	Staat van het product bij ingebruikname	De informatie die de fabrikant op moment van aankoop verstrekte
Kort na de aankoop en ingebruikname	De informatie die de verkoper voor/tijdens de aankoop verstrekte	Staat van het product bij ingebruikname (hoe worden updates aangeboden?)

[63] Goed om hierop te merken is dat met 'de normale consument' niet wordt gedoeld op de juridische 'gemiddelde consument'-maatman (een persoon die bijvoorbeeld ook alle kleine lettertjes leest). In lijn met de meeste consumenten in de praktijk zullen wij eerder tevreden zijn en minder doortastend zijn dan deze maatman.

[64] Indien dit voor de hand ligt worden de foto's pas (direct) na de daadwerkelijke aankoop gemaakt. Het is onnodig om het 'natuurlijke proces' van de aankoop te onderbreken om foto's te maken die ook direct na de aankoop kunnen worden gemaakt.

Moment vergelijking	Welke informatie	Met welke andere informatie
Na iedere veiligheidsupdate	Staat van het product na veiligheidsupdate	De informatie die de verkoper voor/tijdens de aankoop verstrekte
Na afloop van het verder gebruik	De gedurende de testperiode aangeboden updates	De informatie die de verkoper voor/tijdens de aankoop verstrekte

Op basis van de verzamelde informatie zouden ook andere vragen kunnen worden beantwoord (zoals bijvoorbeeld: voldoet de precontractuele informatievoorziening van de verkoper aan de regels?). Deze vragen worden niet door ons beantwoord, maar de informatie uit dit onderzoek wordt wel ter beschikking gesteld (zie Bijlage 6).

Interpretatie van de kenmerken

In het onderzoek is uitsluitend gelet op *aanwezigheid* van een specificatie voor een attribuut. Hoewel is genoteerd wat de verkoper respectievelijk de fabrikant specificeren is in de analyse niet nader gekeken naar de *precisie* van die specificatie. Bij attribuut één en twee (minimumversie Android/iOS) is wel gelet op aanwezigheid van tenminste een ('major') versienummer. We beschrijven in de conclusies ons algemene beeld van de precisie en concreetheid van de specificaties van de kenmerken. Daarnaast hebben we onderzocht of er inhoudelijke verschillen zijn tussen de informatie van verkoper en fabrikant.

Wanneer een specificatie niet eenduidig te bepalen was voor het product (bijvoorbeeld wanneer op de website van de fabrikant specificaties staan die gelden voor een groep producten en we niet kunnen vaststellen dat het onderzochte apparaat deel uitmaakt van deze groep) dan is dit als 'nee' geteld.

3.4 Monitoring informatievoorziening

Voor sommige FCIU-kenmerken is het relevant deze doorlopend te monitoren gedurende de testperiode. Denk hierbij bijvoorbeeld aan de minimumversie van het besturingssysteem van het gebruikersapparaat. Daarnaast ondersteunt de doorlopende monitoring het onderzoek door aanwijzingen te geven over FCIU-kenmerken die mogelijk zijn gewijzigd.

De gemonitorde informatievoorziening omvat een op moment van aankoop vastgestelde set internetpagina's van de verkoper, fabrikant, en enkele door hen gelinkte pagina's, waaronder:

- De productpagina van de verkoper en de productpagina van de fabrikant.
- De App Store/Play Store-pagina van de app behorend bij het product.
- Specifieke pagina's over bijvoorbeeld updates, conformiteitsverklaringen, servicevoorwaarden, handleidingen en FAQ's (met relevante informatie) (criterium: alles gelinkt vanaf de productpagina dat relevant is voor ons onderzoek, dus gerelateerd aan de functionaliteit, compatibiliteit en interoperabiliteit, het updatebeleid en de digitale veiligheid).

We beperken ons tot maximaal vijf links naar de website van de verkoper en maximaal vijf links naar de website van de fabrikant. Wanneer meer relevante links zijn gevonden beperken we ons tot de links die als eerst werden gevonden.

Kort na de aankoop wordt een 'nulmeting' uitgevoerd. Deze nulmeting bestaat uit het (geautomatiseerd) maken van een 'snapshot' van de hierboven beschreven set webpagina's.

3.4.1 Werkwijze bij het maken van een momentopname

Een script bezoekt deze pagina's één voor één, per sessie in een 'schone' browser (Chrome). Ons script 'bestuurt' hierbij de browser. Vanuit het perspectief van de winkel is het in principe lastig, maar theoretisch niet onmogelijk om vast te stellen dat we dit geautomatiseerd doen. We nemen per pagina wachttijd in acht zodat pagina's volledig worden geladen.

Afhankelijk van de domeinnaam van de webpagina passen we specifieke handelingen toe om cookies te accepteren (als niet accepteren ons belemmert om informatie van de site te halen, bijvoorbeeld omdat een cookie-popup over de inhoud heen valt).

We scrollen de hele pagina naar beneden en weer naar boven, om te zorgen dat alle afbeeldingen worden geladen.

We maken vervolgens een 'snapshot' van de pagina in vier vormen:

1. De ruwe broncode pagina (HTML-code) zoals geretourneerd door de webserver bij het ophalen van de URL.
2. De ruwe broncode van de pagina na het volledig laden in de browser
3. De platte tekst op de pagina
4. Een schermafbeelding (in PNG-formaat) van hele pagina.

We doen dit omdat (vanwege complexiteit van de sites) niet altijd alles zichtbaar is op plaatjes. De combinatie van afbeelding en *platte tekst* maakt het mogelijk om (in principe) alle zichtbare inhoud te pakken te krijgen en ook 'in context' te kunnen zien. Ik moet hierbij zeggen dat de websites complex in elkaar zitten en van opbouw kunnen wijzigen. Het volledig 'waterdicht' ophalen van alle informatie is technisch gezien dan ook onmogelijk (maar met deze methode komen we in de praktijk zeer dichtbij).

Voor specifieke pagina's passen we daarna een aantal specifieke handelingen toe, bijvoorbeeld om technische specificaties 'open te klappen' of een tabje aan te klikken. Na iedere specifieke actie wordt opnieuw een snapshot gemaakt zoals hierboven beschreven. Een overzicht van de specifieke handelingen is te vinden in het testlogboek.

Alle snapshots worden opgeslagen in een mappenstructuur (product_X/site_Y/DD-MM-YYY_Z.ext). De eerste snapshot is voorzien van een digitale tijdstempel.

Overige technische details

- Voorafgaand aan het maken van snapshots wordt voor een aantal websites een aantal specifieke handelingen uitgevoerd om de juiste informatie zichtbaar te maken. In veel gevallen moeten cookies worden geaccepteerd om te voorkomen dat de cookie-popup de gezochte informatie bedekte. De acties worden uitgevoerd als 'click'

op een specifiek element binnen de pagina (op basis van CSS-selector[65]), indien dit element bestaat op de pagina. Een overzicht hiervan is te vinden in het testlogboek.

- De dataverzameling vindt in een niet-'headless'[66] browser plaats, omdat sommige websites niet werken in een 'headless'-omgeving.
- Het ophalen van de 'platte tekst'[67] wordt uitgevoerd door voor alle elementen het 'innerText'-attribuut te bepalen en op volgorde van verschijnen in de broncode van de pagina achter elkaar te plakken.
- De schermafbeelding wordt gemaakt met een schermbreedte van 2001 pixels, en hoogte afhankelijk van de inhoud van de pagina. We gebruiken de breedte die door de website wordt aangegeven als voorkeursbreedte, indien beschikbaar.

Onderstaande Figuur 8 toont een voorbeeld van een verschil in de 'platte tekst' van een van de onderzochte websites dat zou kunnen duiden op een wijziging in productspecificaties. Een regel die rood is gemarkeerd is verwijderd, en een groen gemarkeerde regel is ingevoegd ten opzichte van de vorige versie. Alleen gewijzigde (groepen van) regels worden getoond in de context van enkele voorgaande en nakomende regels. De in grijs aangegeven tekst geeft aan op welke locatie in het bestand (regelnummers) de betreffende regels kunnen worden gevonden.

```
120 114 Inclusief lichtbron
121 115 Ja
122 116 Verpakkingsinhoud
123     3 dimbare lampen E27, Radiografische schakelaar, [redacted], Gebruiksaanwijzing.
    117 [redacted] - warm tot koelwit licht - 3 lampen - E27 - 1100lm - 1 dimmer switch
124 118 Productinformatie
125 119 Merk
126 120 [redacted]
        @@ -160,8 +154,10 @@ Minimaal 12 maanden na introductiedatum
160 154 Overige kenmerken
161 155 Aansluitspanning
162 156 230 V
    157 Aantal lichtbronnen
    158 3
163 159 Aantal meegeleverde accu's/batterijen
164     0
    160 Geen
165 161 Bediening verlichting
```

Figuur 8 Voorbeeld van een wijzigingsoverzicht ('diff') van de platte tekst van een webpagina van een verkoper

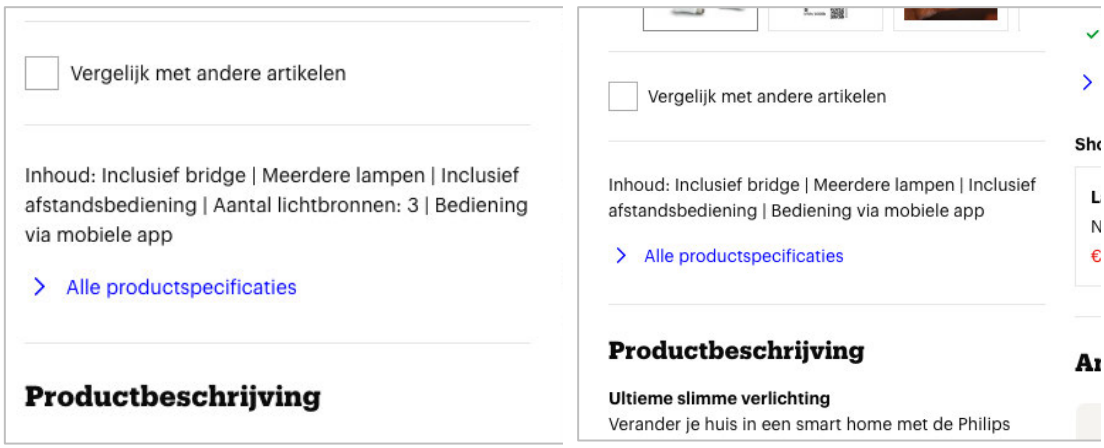
---

[65] Een *CSS-selector* is een manier om een specifiek element of groep elementen op een webpagina aan te duiden op basis van (technische) eigenschappen daarvan. Deze 'selectors' worden normaalgesproken gebruikt binnen websites om specifieke elementen te selecteren waarop bepaalde opmaakregels moeten worden toegepast.

[66] Een *headless browser* is software die functioneert als een webbrowser, maar daarbij de webpagina niet aan een gebruiker laat zien. Deze wordt toegepast bij automatische dataverzameling waarbij het weergeven van de webpagina niet nodig is.

[67] *Platte tekst*: alle tekst op een webpagina die bedoeld is voor weergave aan de bezoeker, ontdaan van lay-out en opmaak.

Van de bijbehorende website is, zoals hierboven beschreven, van beide meetmomenten ook een schermafbeelding beschikbaar. Onderstaande voorbeelden (Figuur 9) tonen een verschil tussen beide versies. Op deze manier kan een verschil in context worden beoordeeld.



Figuur 9 Voorbeeld van een gevonden verschil tussen twee versies van een onderzochte website op basis van schermafbeeldingen.

Onderstaande Figuur 10 toont hoe via een verschil in de 'platte tekst' van een app storepagina relevante wijzigingen in een app kunnen worden opgemerkt.

```
31 31
32 32 What's New
33 33 Version History
34    Feb 28, 2022
   34 Mar 9, 2022
35 35
36    Version 6.34
   36 Version 6.35
37 37
38    Energy IQ: Auto-Assist customers now get a comparison of their energy consumption with the same month last
      accompanied by additional information (e.g. weather, heating time) to better understand their consumption.
   38 • Various UI, stability and performance improvements.
39 39
```

Figuur 10 Voorbeeld van een wijzigingsoverzicht ('diff') van de platte tekst van een webpagina van een verkoper

Archief van verzamelde informatie

Onderdeel van het testrapport is een archief waarin alle verzamelde data is terug te vinden (Bijlage 6).

3.5 Ingebruikname

De ingebruikname van de apparaten gebeurt volgens het volgende stappenplan:

1. Bestickeren en fotograferen van de verpakking van de apparaten
2. Uitpakken, bestickeren en fotograferen van de apparaten
3. Aansluiten van de apparaten
4. Ingebruikname van de apparaten volgens instructies handleiding

We lichten de invulling van de stappen hieronder toe.

3.5.1 Bestickeren en fotograferen van de verpakking van de apparaten

Onderdelen van de verpakking waarop geen informatie is aangebracht (plastic, piepschuim e.d.) worden weggegooid. Alle productverpakkingen worden voorzien van een sticker waarop het productnummer is aangegeven. De sticker wordt geplaatst op een egaal deel van de verpakking waar geen informatie te vinden is.

3.5.2 Uitpakken, bestickeren en fotograferen van de apparaten

De inhoud van de verpakkingen wordt gefotografeerd. Alle losse onderdelen worden voorzien van een sticker waarop het productnummer is aangegeven.

3.5.3 Aansluiten van de apparaten

De apparaten worden aangesloten op elektriciteit. Voor de wasmachines en thermostaten geldt dat zij niet worden verbonden met respectievelijk waterleiding/riolering en een CV-ketel, tenzij duidelijk is dat het apparaat een dergelijke aansluiting nodig heeft om goed te kunnen functioneren.

3.5.4 Ingebruikname van de apparaten volgens instructies handleiding

De apparaten worden in gebruik genomen volgens de in de bijgeleverde handleiding van het product aangegeven stappen.

Koppeling met gebruikersapparaten

Met 'gebruikersapparaat' bedoelen we een smartphone of tablet waarmee het domotica-apparaat kan worden bediend, bijvoorbeeld door daarop een applicatie te installeren. De domotica-apparaten worden (wanneer dat nodig is) gekoppeld met een 'schoon' gebruikersapparaat, welke eveneens verbonden is met het Wi-Fi-netwerk. Hiervoor worden twee gebruikersapparaten gebruikt: een op basis van iOS/iPadOS, en een op basis van Android. Gedetailleerde gegevens van de gebruikte apparaten (waaronder model- en serienummer) staan in Bijlage 5.

De toewijzing van apparaten aan een van beiden geschiedt als volgt: de apparaten worden gesorteerd op aankoopprijs inclusief Btw, hoogste eerst. De oneven apparaten worden met iOS gebruikt, de even apparaten met Android. Mocht het gebruik van het geselecteerde gebruikersapparaat niet mogelijk blijken, dan wordt het andere apparaat gebruikt.

Internettoegang

Alle apparaten worden verbonden met een speciaal hiervoor ingericht (Wi-Fi-)netwerk. Op dit netwerk zijn alle apparaten gelijktijdig aangesloten.

Het netwerk biedt onbeperkte toegang tot het internet op basis van IPv4 via een VPN-verbinding. Er is geen firewall actief op de verbinding; wel wordt er gebruik gemaakt van NAT, en zijn inkomende poorten initieel gesloten.

De internetverbinding verloopt over een zakelijke glasvezelaansluiting met een beschikbaarheid van meer dan 99% (incidenten die tijdens de testperiode optreden worden gelogd in het testrapport). De bandbreedte van deze verbinding is gemaximeerd op 50 Mbit/s in zowel de down- als upstream. Het publieke IP-adres is Nederlands. Deze situatie lijkt op een thuissituatie waarbij een door een ISP geleverde modemrouter wordt gebruikt.

Alle communicatie met het internet en tussen apparaten op het netwerk wordt lokaal gelogd. Deze logs worden gearchiveerd.

3.6 Analyse functionaliteit, compatibiliteit, interoperabiliteit, updatebeleid

In deze stap analyseren we de geselecteerde concrete FCIU-kenmerken (Tabel 1) van de apparaten. Deze stap vindt op verschillende momenten plaats: allereerst tijdens de ingebruikname, en vervolgens na iedere update van de apparaatsoftware (*herhaling*).

Merk hierbij op dat niet alle FCIU-kenmerken op beide soorten meetmomenten zijn geïnventariseerd. Bij *herhaling* controleren we attribuut 3 en attributen en 7 t/m 16 (zie Tabel 1). Van attribuut 4 (de ondersteunde Wi-Fi-frequenties) is het niet aannemelijk dat deze wijzigt door een software-update (deze is daarom bij herhaling niet expliciet gecontroleerd, maar een wijziging op dit vlak zou wel direct opvallen in de testomgeving en dan uiteraard worden gerapporteerd). Attributen 5 en 6 (de minimumtermijn van de updates) staan eveneens los van updates van de apparaatsoftware zelf.

Attributen 1 en 2 (de minimumversie van het besturingssysteem van het gebruikersapparaat waarop de bijbehorende app werkt) zijn relevant om te controleren na een update van de *app*. Deze attributen zijn bij ingebruikname en op de laatste dag van de testperiode gemeten (voor de versies van de apps die op dat moment in gebruik waren).

In aanvulling op de FCIU-kenmerken uit Tabel 1 worden ook alle door de onderzoekers eventueel opgemerkte substantiële wijzigingen van FCIU-gerelateerde eigenschappen die *niet* in de lijst zijn opgenomen gerapporteerd. Daarnaast rapporteren we over eventuele verschillen tussen FCIU-'claims' op de verpakkingen en/of andere bijgevoegde materialen en de gevonden feitelijke en verstrekte informatie over FCIU-kenmerken. Hierbij is gelet op zinnen/zinsneden of bijvoorbeeld logo's of keurmerken op de verpakking.

3.7 Analyse digitale veiligheid aan de hand van vereisten

In dit onderzoek toetsen we de apparaten aan normen en 'good practices' vanuit een normenkader voor digitale veiligheid. Dit schept een goed beeld van het niveau van de digitale veiligheid van de apparaten. De analyse van digitale veiligheid bestaat uit een nulmeting en een meting na updates van de apparaatsoftware.

3.7.1 Afbakening en uitgangspunten

De analyse van digitale veiligheid wordt uitgevoerd vanuit het perspectief van een kwaadwillende die via internet op afstand toegang wenst te verkrijgen tot het onderzochte apparaat (met als doel deze te schakelen, onderdeel te maken van een *botnet*, te gebruiken als *foothold*[68], gegevens van de gebruiker te stelen, et cetera). Dit heeft de volgende gevolgen voor de reikwijdte van het beveiligingsonderzoek (in lijn met de onderzoeksopdracht):

- De security-analyse betreft in beginsel alleen het apparaat zélf. Daarvan onderzoeken we initieel het deel dat (via een lokaal netwerk) toegang heeft tot internet. Bij een combinatie van domotica-hub en -lamp zal het onderzoek zich initieel richten op de domotica-hub, daar dit het element is dat is aangesloten op een lokaal netwerk met internettoegang. Zwakheden in lokale netwerkinterfaces (zoals ZigBee of Bluetooth) vallen buiten scope, omdat dit niet zonder meer exploiteerbaar is via internet.

[68] Een *foothold* is een door een aanvaller verkregen vorm van toegang tot een digitaal systeem, met behulp waarvan deze toegang kan (proberen te) krijgen tot andere onderdelen of digitale systemen.

- De clouddienst van een aanbieder valt *niet* binnen het bereik van de security-analyse. Wanneer het apparaat op een veilige wijze verbinding maakt met een dergelijke dienst (inclusief authenticatie) wordt veiligheid van deze dienst aangenomen. De veiligheid van deze communicatie wordt uiteraard wel meegenomen.

- De app die nodig is om het apparaat te installeren en/of gebruiken valt buiten het bereik. Hoewel de app zou kunnen worden misbruikt door een aanvaller vraagt dit toegang tot het gebruikersapparaat (en zou analyse dus vooral leiden tot inzichten over de veiligheid van het gebruikersapparaat). Uiteraard wordt wel gekeken naar de *interface* tussen de app en het apparaat; als deze onveilig is zou deze uiteraard kunnen worden misbruikt door een aanvaller met toegang tot het lokale netwerk. Daarnaast valt het *updatemechanisme* van de apparaten, wat mogelijk via de app loopt, binnen het bereik. Als het dus voor een aanvaller mogelijk is om (bijvoorbeeld) verkeer tussen de applicatie en de update-server tijdens het downloaden en installeren van een update te manipuleren, dan is dit binnen scope.

- De integriteit van de apparaten wordt niet aangetast. Dit betekent dat er geen wijzigingen worden uitgevoerd aan de hardware (anders dan op instructie van de handleiding) noch aan de software. Wel worden indien mogelijk instellingen van het gebruikersapparaat gewijzigd om afluisteren van het netwerkverkeer mogelijk te maken (zie verderop).

3.7.2 Normenkader

Voor de security-analyse zullen de technische eisen vanuit het normenkader "IoT Assurance Framework 3.0" d.d. november 2021 [18] (hierna 'IoTSF') en de *"essential security requirements for consumer IoT devices"* van Qbit [19] worden gebruikt als referentiekader.

Het *IoT Security Assurance Framework* is een praktische hulpbron die IoT-leveranciers helpt om hun producten en diensten op de juiste manier te beveiligen. Het is een veelzijdige publicatie die fungeert als een gids, een hulpmiddel en een referentie voor deskundigen. De publicatie leidt gebruikers door een risicobeheerproces om beveiligingsdoelstellingen te bepalen en biedt een sjabloon voor het verzamelen van bewijsmateriaal om beveiligingsclaims te helpen aantonen. Doelgericht bewijs kan vervolgens worden gebruikt ter ondersteuning van zakelijke behoeften in commerciële (klant), conformiteit(snormen) of compliance (regelgeving) omgevingen.

Qbit [19] geeft, op basis van een meta-analyse van verschillende raamwerken voor security voor IoT-devices, een zevental "essentiële vereisten" waaraan een IoT-apparaat gericht op consumenten minimaal zou moeten voldoen. Omdat het hier gaat om minimumvereisten is ervoor gekozen om naast deze vereisten een uitgebreider raamwerk te hanteren, waaruit (voor de hier onderzochte productsoorten relevante) relevante vereisten worden geselecteerd. Hiervoor is in eerste instantie gekozen voor het IoT Assurance Framework 3.0 dd. november 2021 [18].

Zoals uit de labeling in Bijlage 2 duidelijk wordt is er een hoge mate van overlap tussen de Qbit-vereisten en relevante vereisten uit het IoTSF.

Alternatieve normenkaders

Andere relevante normen die zouden kunnen worden gebruikt als uitgangspunt zijn (onder andere) EN 303 645 [20] en ISO-27403 [21]. Nadere inhoudelijke analyse van deze normen leert dat de gestelde vereisten vrijwel volledig overlappen met de uit het IoTSF geselecteerde vereisten.

3.7.3 Uitwerking

In een periode van drie maanden zullen iedere twee weken een analyse van netwerkverkeer en geautomatiseerde penetratietesten en kwetsbaarhedenscans op de apparaten worden uitgevoerd. De analyse van het netwerkverkeer geeft inzicht in de exfiltratie van informatie[69], geautomatiseerd downloaden en toepassen van updates en kan informatie geven over het gebruik van kwetsbare softwarebibliotheken. Tijdens deze analyse zullen gebruikte softwarecomponenten opnieuw worden geïnventariseerd en zal worden gekeken of publiek bekend zwakheden (CVE[70]'s) zijn geconstateerd binnen deze componenten. Naast het toetsen van de het beveiligingsniveau over een langere periode en gedurende de werking van het apparaat voorziet deze fase ook het onderzoeksteam van een overzicht van relevante wijzigingen. Aan de hand van de wijzigingen kunnen additionele onderzoeken worden verricht om zo risicogebaseerd het onderzoek van meer diepgang te voorzien. De resultaten vanuit deze fase worden eveneens opgenomen in de conceptrapportage.

De geselecteerde technische eisen en de wijze waarop deze worden getest zijn te vinden in Bijlage 2. Op hoofdlijnen worden per analyse de volgende acties uitgevoerd:

- Poortscan (o.b.v. nmap[71] en vergelijkbare tools)
- Kwetsbaarhedenscan (o.b.v. Nessus[72] en vergelijkbare tools)
- Specifieke geautomatiseerde tests om een groot deel van de eisen vanuit het normenkader te toetsen (zie Bijlage 2).
- Analyse van het netwerkverkeer. De analyse van het netwerkverkeer geeft inzicht in de exfiltratie van informatie, geautomatiseerd downloaden en toepassen van updates en kan informatie geven over het gebruik van kwetsbare softwarebibliotheken.
- Analyse ten opzichte van de CVE-database.

Op basis van resultaten vanuit de analyse van het netwerkverkeer en de geautomatiseerde penetratietesten worden analyses van digitale veiligheid uitgevoerd op individuele apparaten. Deze additionele analyse zal worden uitgevoerd na een update of andere (significante) wijzigingen aan het apparaat. Als apparaten in een vroeg stadium al niet meer blijken te voldoen aan huidige *security good practices* (op basis van de eerder toegelichte vereisten) zal met meer diepgang worden gekeken naar de overige apparaten.

---

[69] *Gegevensexfiltratie* vindt plaats wanneer malware en/of een kwaadwillende actor een ongeautoriseerde gegevensoverdracht vanaf een computer uitvoert. Het wordt ook vaak data-extrusie of data-export genoemd.

[70] *Common Vulnerabilities and Exposures* (CVE) is een databank met informatie over kwetsbaarheden in computersystemen en netwerken.

[71] *Nmap* ("Network Mapper") is een gratis en open source hulpprogramma voor netwerkverkenning en beveiligingscontrole.

[72] *Nessus* is een computerprogramma dat gebruikt wordt om de beveiliging van computers en computernetwerken na te gaan.

Hierdoor wordt een verdiepingsslag aangebracht in het onderzoek en zal een beter inzicht worden verkregen in de verschillende beveiligingsniveaus. Resultaten van de onderzoeken en invloed op de compliance met het normenkader zullen worden opgenomen in de conceptrapportage en tussentijds worden gerapporteerd.

Binnen deze additionele security-analyse zullen de volgende acties worden uitgevoerd:

- Manuele penetratietest;
- Manuele analyse van het netwerkverkeer;
- Manuele security review van het apparaat.

Gedurende deze acties zullen minimaal de vereisten uit het normenkader worden getoetst. Andere beveiligingsrisico's die niet kunnen worden gerelateerd aan het normenkader zullen als opmerking worden meegenomen in het testrapport.

Analyse op basis van CVE's

Voor iedere dienst die benaderbaar is via het lokale netwerk zal worden getoetst of een zwakheid aanwezig is. Het toetsen op zwakheden gebeurt initieel op basis van de informatie die wordt geretourneerd door de dienst, bijvoorbeeld versienummers, specifieke headers en specificaties van gebruikte softwarecomponenten. Daarnaast zal ook een kwetsbaarheden- en webapplicatiescan worden uitgevoerd. Op basis van deze informatie zullen eventueel CVE's worden gerelateerd aan de zwakheden die zijn geconstateerd. Hierbij gaat het in principe om alle CVE's die op het moment van testen bekend zijn en zal ook een *false positive* verificatie plaatsvinden. Het resultaat van deze analyse is een lijst met CVE's gekoppeld aan de apparaten waarop de betreffende zwakheden aanwezig zijn.

Per apparaat wordt in openbare databases (welke zijn samengevoegd in een interne database door CREDS) gezocht naar CVE's (meldingen van zwakheden). Het zoeken van CVE's vindt plaats op basis van 'Common Platform Enumeration strings' (hierna: CPE-strings). [22] CPE-strings beschrijven eigenschappen van onderliggende hardware en software. Door te zoeken op basis van CPE-strings kan een zwakheid worden gevonden in de CVE-database die betrekking heeft op (bijvoorbeeld) een softwarebibliotheek die een product gebruikt, zonder dat in de database specifiek is aangegeven dat de zwakheid ook op het specifieke product van toepassing is.

3.7.4 Technische inrichting

De apparaten worden aangesloten op een speciaal ingericht Wi-Fi-netwerk waarop alleen de onderzochte apparaten en de gebruikersapparaten zijn aangesloten. Dit netwerk gedraagt zich in alle opzichten zoals een thuisnetwerk (dat wil zeggen: nagenoeg[73] onbeperkte toegang tot het internet via IPv4, gebruik makend van NAT). Het netwerk wordt gerealiseerd met een mini-PC, welke in de testruimte aanwezig is.

Er wordt gebruik gemaakt van een Nederlands publiek IP-adres dat niet voor andere doeleinden wordt gebruikt gedurende het onderzoek, en niet is gebruikt in 2021 (maar gedurende die periode wel ter beschikking stond aan de onderzoekers).

Apparaten die geen Wi-Fi ondersteunen worden via Ethernet aangesloten. Het ethernetsegment is hetzelfde als het Wi-Fi-segment. Apparaten die verbonden zijn via Wi-Fi kunnen met apparaten communiceren die via Ethernet zijn verbonden, en andersom. Dit

[73] De meeste consumentenproviders blokkeren enkele poorten (waaronder poort 25, gebruikt voor uitgaand e-mailverkeer) en staan toegang tot bepaalde servers niet toe (op basis van hostnaam via DNS-blokkades, en/of door blokkade van verkeer naar bepaalde IP-adressen).

verkeer wordt eveneens gemonitord.[74] De gebruikersapparaten worden via Wi-Fi aangesloten.

Man-in-the-middle

Om analyse van het netwerkverkeer te kunnen uitvoeren wordt gebruik gemaakt van een 'man in the middle'-proxy (PolarProxy). Deze onderschept het verkeer tussen (1) het gebruikersapparaat en het apparaat, (2) het apparaat en het internet, en (3) het gebruikersapparaat en het internet. Verkeer dat is versleuteld wordt onderschept en gedecodeerd. Om dit mogelijk te maken wordt een zogenaamd 'rootcertificaat' geïnstalleerd op het gebruikersapparaat. Voor apparaten die zelfstandig met het internet communiceren is het toevoegen van dit rootcertificaat meestal niet mogelijk (en een aantasting van de integriteit ervan – zie paragraaf 3.7.1).

Wanneer het apparaat en/of de applicatie dienst weigert omdat het verkeer wordt onderschept (via het eigen 'rootcertificaat') wordt het apparaat en/of de dienst waarmee deze gecommuniceerd 'gewhitelist'. Dit wil zeggen dat de proxysoftware geen pogingen meer doet om het verkeer met deze dienst / vanaf dit apparaat te ontsleutelen. Het feit dat een applicatie maatregelen neemt om het gebruik van een eigen rootcertificaat tegen te gaan ("certificate pinning") is overigens op zichzelf een positieve uitkomst van dit onderzoek.

Remote access

Voor het uitvoeren van penetratietesten wordt gebruik gemaakt van een (deels) geautomatiseerd platform en diverse tools (zie ook Bijlage 2). Deze tools worden uitgevoerd vanuit een cloudomgeving. Via deze omgeving hebben de onderzoekers ook op afstand toegang tot het testlab. Het testnetwerk is via een veilige, afgeschermde VPN-verbinding met deze omgeving verbonden.

3.8 Gebruik van het apparaat

De apparaten worden minimaal gebruikt. Doel van dit gebruik is om te zorgen dat de apparaten (periodiek of doorlopend) ingeschakeld zijn en de kans krijgen om automatische updates uit te voeren, om FCIU-kenmerken en digitale veiligheid te kunnen controleren, en om updates te installeren.

Niet alle apparaten zullen continu ingeschakeld zijn noch voortdurend verbinding met het Wi-Fi-netwerk behouden. De apparaten die niet voortdurend verbinding hebben met het Wi-Fi-netwerk zullen we dagelijks inschakelen ('uit stand-by halen') en ingeschakeld laten totdat zij zich automatisch uitschakelen.

Functies die potentieel veel bandbreedte gebruiken (zoals het downloaden van screensavers op smart-TV's) schakelen we uit om de verkeerslogging niet te overbelasten. We doen dit alleen wanneer overduidelijk is dat het verkeer voor onze analyse niet relevant is om bij te houden. We maken hier een aantekening van in het testrapport.

[74] Om technische redenen wordt verkeer *tussen* apparaten op het ethernetsegment niet worden gemonitord. Verkeer tussen Wi-Fi-apparaten, waaronder in het bijzonder met het gebruikersapparaat, wordt uiteraard wel gemonitord.

3.8.1 Update-regime

Vanaf de ingebruikname tot het einde van de testperiode voeren we updates op de apparaten door. In het testrapport houden we de datum/tijd en softwareversie na iedere update bij. Voor het initiëren van de updates volgen we het onderstaande regime:

Tijdens ingebruikname

- Wanneer het apparaat (c.q. de app) tijdens ingebruikname voorstelt een update te installeren, dan zullen we dit toestaan.
- Wanneer het apparaat (c.q. de app) tijdens ingebruikname vraagt of automatische updates moeten worden ingeschakeld, dan zullen we dit inschakelen.

Na afloop van de ingebruikname wordt de actuele versie van de software genoteerd (zoals aangegeven in de app/het menu van het apparaat).

Na ingebruikname, voor einde beveiligingstest

We installeren geen handmatige updates. Wel wordt dagelijks op werkdagen[75] gekeken of er updates worden aangeboden of automatisch zijn geïnstalleerd.

Tijdens gebruiksperiode

Wij controleren dagelijks (op werkdagen) of het apparaat (c.q. de app) aangeeft dat er een update is (via het menu, de app, of via een pushbericht op de smartphone). Zo ja zullen wij de update starten. We noteren na iedere update de geïnstalleerde versie van de software.

Wanneer een update (automatisch of handmatig geïnitieerd) is misgegaan zullen we deze zo snel mogelijk opnieuw proberen te installeren. We doen dit per updateversie maximaal twee keer.

3.8.2 Update-regime gebruikersapparaat

Op het gebruikersapparaat zijn automatische updates van het besturingssysteem ingeschakeld. Bij aanvang van de testperiode was op de apparaten de meest recente beschikbare en voor het apparaat geschikte versie van het besturingssysteem geïnstalleerd.

3.9 Analyse veiligheid updatemethodiek

De apparaten worden via een speciaal ingericht Wi-Fi-netwerk verbonden met internet (zie paragraaf 3.5). Alle communicatie tussen het apparaat en het internet, het gebruikersapparaat en het internet, en tussen het apparaat en het gebruikersapparaat wordt gemonitord. Met behulp van deze gegevens kan worden vastgesteld op welke wijze het apparaat updates controleert, downloadt en installeert.

Primair letten we op de poorten en protocollen waarmee het apparaat online updates aanvraagt en ophaalt (naar verwachting bij de fabrikant). Op basis van standaardtools (onder andere Wireshark[76]) kan worden gedetecteerd op basis van welke protocollen wordt

[75] Maandag tot en met vrijdag, met uitzonderingen van nationale feestdagen.

[76] Wireshark is software waarmee netwerkverkeer kan worden opgeslagen en geanalyseerd.

gewerkt. We verwachten dat er voornamelijk HTTPS-verbindingen[77] zullen worden gebruikt.

HTTPS-verbindingen zijn in principe niet 'af te luisteren'. Omdat we ook geïnteresseerd zijn in de vraag of aangevraagde updates door het apparaat worden geauthentiseerd (zie Bijlage 2) proberen we als 'man in the middle' in het verkeer in te kijken. We installeren hiervoor een door ons gegenereerd rootcertificaat op het gebruikersapparaat (en, als de mogelijkheid wordt geboden, ook op het apparaat zelf). Wanneer het rootcertificaat niet wordt herkend door het apparaat zal deze (als het goed is) weigeren verbinding te maken.

3.10 Uitzonderingssituaties

3.10.1 Een apparaat raakt defect gedurende de testperiode

Voor apparaten die defect (lijken te) zijn gedurende de testperiode volgen we de in de bijgeleverde handleiding aangegeven instructies. Als de handleiding dit niet al voorschrijft zullen we vervolgens een poging doen de fabrieksinstellingen te herstellen en het apparaat opnieuw in gebruik te nemen. Wanneer een apparaat onherstelbaar is eindigt het onderzoek voor dit apparaat.

3.10.2 Een apparaat raakt besmet/wordt gehackt gedurende de testperiode

Wanneer we constateren dat een apparaat besmet is geraakt met malware en/of is gehackt gedurende de testperiode, volgen we de volgende procedure:

1. We constateren de hack/malware. We melden dit direct aan de opdrachtgever.
2. We onderzoeken wat er precies is gebeurd en noteren dit in het testrapport.
3. We herstellen het apparaat naar de fabrieksinstellingen en nemen het opnieuw in gebruik.
4. Wanneer herbesmetting optreedt eindigt het onderzoek voor dit apparaat en koppelen we het apparaat los.

3.10.3 We ontdekken een zwakheid in de beveiliging van een van de apparaten

Wanneer we een zwakheid ontdekken in een van de apparaten zoeken we allereerst uit of de fabrikant een beleid voor *coordinated vulnerability disclosure* (of voorheen gangbaar: *responsible disclosure)* hanteert. Een dergelijk beleid beschrijft de gecontroleerde overdracht en vrijgave van informatie over beveiligingszwakheden, zodat misbruik ervan kan worden geminimaliseerd. In dit beleid is aangegeven hoe de fabrikant meldingen wil ontvangen van beveiligingszwakheden. We melden vervolgens de zwakheid bij de fabrikant volgens de voorkeursroute. De tekst leggen we vooraf voor aan de opdrachtgever.

Uiteraard is relevant of de fabrikant de zwakheid oplost en dit leidt tot een update (dit merken we op zolang de update binnen de testperiode wordt uitgebracht).

Mocht op moment van publicatie de zwakheid niet zijn opgelost, dan zal een afweging worden gemaakt of en zo ja, op welke wijze, de details van de zwakheid kunnen worden

[77] HTTPS verwijst naar de combinatie van HTTP (het Hypertext Transfer Protocol) en TLS (het Transport Layer Security-protocol). Met TLS kunnen netwerkverbindingen worden vercijferd en kunnen de communicerende partijen elkaar authenticeren. Met HTTP kan worden geïnteracteerd met websites. HTTPS wordt gebruikt om links te kunnen bezoeken die beginnen met 'https://'.

opgenomen in het (mogelijk uiteindelijk geheel of deels openbaar gepubliceerde) testrapport.

3.11 Beperkingen van de methode

De onderzoeksmethode kent een aantal beperkingen. De volgende kanttekeningen zijn van belang bij interpretatie van resultaten die op basis van de methode verkregen zijn:

- **De meting betreft een momentopname onder zeer specifieke omstandigheden**. Hoewel de onderzoekers zorgvuldig te werk gaan is het niet volledig uit te sluiten dat de uitkomsten bij herhaling van het onderzoek afwijken. Een en ander zou kunnen worden veroorzaakt door het grote aantal stappen en interacties met de apparaten, alsook het grote aantal omgevingsvariabelen, zoals de gebruikte randapparatuur.[78] Daarnaast is het denkbaar dat er verschillen zijn tussen de software van twee apparaten, zelfs wanneer het versienummer overeenkomt, bijvoorbeeld wanneer de fabrikant 'hotfixes'[79] of A/B-testing[80] toepast, updates heeft teruggetrokken of meerdere verschillende versies uit heeft gebracht met hetzelfde versienummer[81]). Voor deze omstandigheden kan (binnen het geschetste onderzoekskader en -budget) niet volledig worden gecontroleerd. Zo is in de afbakening van het onderzoek bepaald dat de integriteit van de apparaten niet wordt aangetast. Zodoende is bijvoorbeeld niet te bepalen welke software er *exact* op het apparaat draait, en moeten we afgaan op het gerapporteerde versienummer.

- **Voor veel van de hier onderzochte zaken geldt dat het (theoretisch en praktisch gezien) niet mogelijk is om 100% uitsluitsel te geven.** Bij veel onderzochte aspecten gaat het om aan- of afwezigheid van een bepaald kenmerk (bijvoorbeeld een beveiligingslek). Hierbij geldt het credo *"afwezigheid van bewijs is geen bewijs van afwezigheid":* Hoewel we (volgens de hierboven beschreven methode) trachten om aan- of afwezigheid van bepaalde eigenschappen met de hoogst mogelijke zekerheid vast te stellen, is volledige zekerheid niet te geven. **Een positieve score op het aspect digitale veiligheid betekent daarom ook niet dat het apparaat volledig digitaal veilig is**.

- Bij de informatieverstrekking kijken we naar de aan ons verstrekte materialen en beschikbare specifieke (web)pagina's op specifieke meetmomenten. Het is uiteraard

---

[78] Omdat de apparaatsoftware zélf niet is geanalyseerd (in dit onderzoek is ervoor gekozen de apparaatintegriteit niet te schenden) is niet met zekerheid te stellen dat apparaatsoftware geen code bevat die alleen in specifieke omstandigheden word uitgevoerd.

[79] Met *hotfixes* bedoelen we ad-hoc updates van de apparaatsoftware die buiten de reguliere updatecadans worden uitgebracht, bijvoorbeeld om een specifiek probleem, eventueel voor een specifiek deel van de apparaten, op te lossen.

[80] Bij *A/B-testing* worden twee of meer alternatieven (bijvoorbeeld op het gebied van de gebruikersinterface of implementatie van een functie) tegelijkertijd uitgerold. Per gebruiker wordt (meestal willekeurig) een van de alternatieven geactiveerd. Door te kijken naar de gevolgen op bijvoorbeeld het gebruik en de tevredenheid van de gebruiker kan vervolgens worden bepaald welk alternatief uiteindelijk de hoofdimplementatie wordt. Er kunnen tegelijkertijd meerdere A/B-tests worden uitgevoerd. In dat geval neemt het aantal unieke combinaties van geactiveerde implementaties exponentieel toe.

[81] Het toewijzen van versienummers is naar keuze van de ontwikkelaar. Technisch gezien is het mogelijk om hetzelfde versienummer toe te kennen aan verschillende versies van apparaatsoftware. Omdat de apparaatsoftware in dit onderzoek niet is geëxtraheerd uit de apparaten is niet met volledige zekerheid vast te stellen dat hetzelfde versienummer niet is hergebruikt.

mogelijk dat de verkoper of fabrikant op andere locaties informatie publiceren die (toevalligerwijs of als gevolg van de gevolgde procedure) niet is gevonden. Verkopers, fabrikanten en aanbieders van zoekmachines kunnen informatie op hun websites te allen tijde, waaronder gedurende het onderzoek, wijzigen.

4 Resultaten

In dit hoofdstuk presenteren we de resultaten op basis van de steekproef van domotica-apparaten. We bespreken in dit hoofdstuk de resultaten op hoofdlijnen, om zo een algemeen beeld van de steekproef te beschrijven. Gedetailleerde resultaten per apparaat zijn te vinden in Bijlage 3.

4.1 Voorbereidende fase

In de voorbereide fase wordt een selectie gemaakt van onderzochte FCIU-kenmerken en apparaten. De selectie van kenmerken wordt toegelicht in het methodehoofdstuk (paragraaf 3.1). Hieronder lichten we de uitkomsten van de apparaatselectie toe.

4.1.1 Apparaatselectie

De in paragraaf 3.2 beschreven methode voor productselectie is toegepast en leidde tot een selectie van 15 apparaten. De basisgegevens van deze apparaten zijn te vinden in Tabel 4 op de volgende pagina.

Merk op dat in twee gevallen de winkel zelf niet de verkoper is (in juridische zin). De apparaten worden door de verkoper aangeboden in een online winkel waar ook andere verkopers apparaten aanbieden (een *tussenhandeldienst*) In Tabel 4 is in deze gevallen de naam van de winkel en tussen haken de naam van de verkoper gegeven.

4.2 Aankoopfase

Voorafgaand en tijdens het aankopen van de apparaten is een archief opgesteld met informatie zoals door verkoper en fabrikant verstrekt (zie testmethodiek). Op basis van deze archieven is vervolgens voor de FCIU-kenmerken (Tabel 1) bepaald of deze werden gespecificeerd in de informatie van respectievelijk de verkoper en de fabrikant.

4.2.1 Precontractuele informatie verstrekt door de verkoper

Onderstaande Tabel 5 toont de mate waarin verkopers precontractueel informatie over de door ons gecontroleerde FCIU-kenmerken verschaften voor de onderzochte apparaten. Deze tabel is gebaseerd op de productpagina's van de verkopers en een aantal geselecteerde andere pagina's van de verkoper (nadere analyse van algemene voorwaarden is separaat uitgevoerd en wordt hieronder toegelicht). Een overzicht van de geanalyseerde pagina's is te vinden in Bijlage 4.

Verkoper, winkel, of beide?

Voor twee online gekochte apparaten was de verkoper (in juridische zin) een andere organisatie dan de exploitant van de online winkel waarbinnen het product werd aangeboden en gekocht. Het is daarbij niet altijd duidelijk van wie de productinformatie afkomstig is.

Tabel 4 Basisgegevens geselecteerde en onderzochte apparaten

ID	Korte naam in dit rapport	Productcategorie	Verkoop kanaal	Winkel [Verkoper]	Merknaam	Volledige productnaam	Prijs (incl. Btw)	Productpagina verkoper
1		Domotica-hub met gekoppelde slimme lamp	Online					Link
2		Domotica-hub met gekoppelde slimme lamp	Online					Link
3		Domotica-hub met gekoppelde slimme lamp	Offline					Link
4		Slimme babyfoon	Online					Link
5		Slimme babyfoon	Online					Link
6		Slimme babyfoon	Online					Link
7		Smart tv	Online					Link
8		Smart tv	Online					Link
9		Smart tv	Offline					Link
10		Slimme thermostaat	Offline					Link
11		Slimme thermostaat	Online					Link
12		Slimme thermostaat	Offline					Link
13		Slimme wasmachine	Online					Link
14		Slimme wasmachine	Online					Link
15		Slimme wasmachine	Offline					Link

Precontractueel verstrekte informatie bij offline aankopen

Merk op dat deze analyse de *online* verstrekte informatie betreft, ook voor apparaten die 'offline' zijn gekocht. De in de fysieke winkel verstrekte informatie liep sterk uiteen en bleek op de meeste punten niet precies genoeg. Daarnaast is de kwaliteit en concreetheid van de verstrekte informatie sterk afhankelijk gebleken van de kennis van de desbetreffende verkoper in de winkel. Zo staat in een van de verslagen: *"Medewerker weet niet hoe lang updates gegarandeerd zijn, maar geeft aan dat het een nieuw apparaat is".* Bij de onderzoekers die de aankoop deden wekte dit naar hun mening de indruk dat het apparaat 'nog wel even' ondersteund zal worden. In een ander verslag werd benoemd *"dat het niet zo is dat binnen tien jaar die lamp er niet meer op werkt."* In een andere winkel werd verwezen naar de website van de winkel en werd de website van de fabrikant van het desbetreffende product samen met de koper bekeken. In weer een andere winkel bleek de medewerker in kwestie veel te weten over een product, naar eigen zeggen omdat de medewerker het product zelf ook gebruikt.

Gezien de variatie van de kwaliteit van informatieverstrekking en de slechte verifieerbaarheid van de informatie concluderen we dat het niet valide is om op basis van deze metingen generaliseerbare (voor de winkel, het product, en/of offline verkoop van domotica-apparaten in het algemeen) conclusies te trekken.

Voor deze analyse kiezen we ervoor om ons te baseren op de online door deze winkels verstrekte informatie. Daarmee is uiteraard niet gezegd dat deze informatie (juridisch gezien) als vervanging moet worden gezien voor de offline verstrekte informatie. Wel komt de set beoordeelde informatie overeen met de informatie die zou zijn beoordeeld voor de aankoop, mocht deze online zijn uitgevoerd binnen dit onderzoek. De resultaten die we voor deze apparaten presenteren kunnen niet worden gebruikt om vast te stellen of aan de precontractuele informatieverplichtingen binnen de verkoopruimte is voldaan. We geven de resultaten in de betreffende overzichten dan ook gescheiden weer.

4.2.2 Precontractuele informatie verstrekt door de fabrikant

Tabel 6 toont de mate waarin fabrikanten op moment van aankoop informatie over de door ons gecontroleerde FCIU-kenmerken verschaften voor de onderzochte apparaten. Deze tabel is gebaseerd op de productpagina's van de fabrikanten en een aantal andere pagina's van de fabrikanten (selectie op basis van de procedure als beschreven in hoofdstuk 3). Een overzicht van de geanalyseerde pagina's is te vinden in Bijlage 4. Nadere analyse van algemene voorwaarden is separaat uitgevoerd en lichten we hieronder toe.

Hoe lang blijft de dienst van de fabrikant (en eventueel andere relevante diensten) actief?

In deze analyse is gekeken naar de FCIU-kenmerken zoals beschreven in het methodologiehoofdstuk.

Een kenmerk dat niet was gedefinieerd is de termijn waarbinnen de dienst van de fabrikant ten behoeve van het apparaat minimaal beschikbaar blijft. Voor de apparaten waarbij een clouddienst nodig is (voor het gebruik van specifieke 'smart'-functies) werd voor geen van de apparaten, door de verkoper noch fabrikant, aangegeven hoelang deze clouddienst in de toekomst actief blijft. Gezien de sterke afhankelijkheid van deze diensten van veel van de onderzochte apparaten lijkt ons dit een relevant attribuut om toe te voegen. In de praktijk zien we (bijvoorbeeld bij *multiplayer*-games) dat de ondersteuning voor dergelijke diensten op enig moment wordt beëindig (zie bijvoorbeeld

[23] en [24]) Dat zou bij veel van de onderzochte apparaten kunnen betekenen dat functionaliteit wegvalt.

Juridisch gezien zou de verkoper daarmee echter aansprakelijk zijn, aangezien de consument niet gedurende een redelijkerwijs te verwachten periode (die in relatie staat tot een redelijk te verwachten levensduur van het apparaat) ongestoord gebruik kan maken van de geleverde zaak (art. 7:18 lid 2 onder a en d en lid 4 BW). Dit is mogelijk anders indien de verkoper de consument hierover uitdrukkelijk heeft geïnformeerd en de consument met deze afwijking uitdrukkelijk en afzonderlijk heeft ingestemd (art. 7:18 lid 6 BW).[82]

4.2.3 *Precontractuele informatie verstrekt door de verkoper versus fabrikant*

Tabel 12 (in Bijlage 3) toont de verschillen tussen de informatieverstrekking door de fabrikant en verkoper. Hiertussen vinden we enkele relevante verschillen:

- In 31 gevallen werd door de verkoper géén informatie verstrekt over een FCIU-kenmerk terwijl de informatie wel werd verstrekt door de fabrikant.
- In 17 gevallen werd door de fabrikant géén informatie verstrekt over een FCIU-kenmerk terwijl de informatie wel werd verstrekt door de verkoper.
- In twee gevallen verschilt de informatie die de verkoper verstrekt evident van de informatie die de fabrikant verstrekt. In het ene geval ging het om een verschil in de minimaal ondersteunde Android-versie, en in het andere geval ging het om een verschil in de minimaal ondersteunde iOS-versie van de bijbehorende app.

Merk bij de tabellen op dat de minimumversie van de bijbehorende iOS-app voor alle apparaten (waarvoor de app is meegenomen in de test) beschikbaar was. De reden hiervoor is dat de minimumversie door Apple altijd wordt weergegeven in de App Store, en deze pagina's mee zijn genomen in de set fabrikantinformatie. Voor apparaat 9 ontbreekt informatie van de fabrikant, omdat voor dit product geen productpagina kon worden gevonden van de fabrikant.

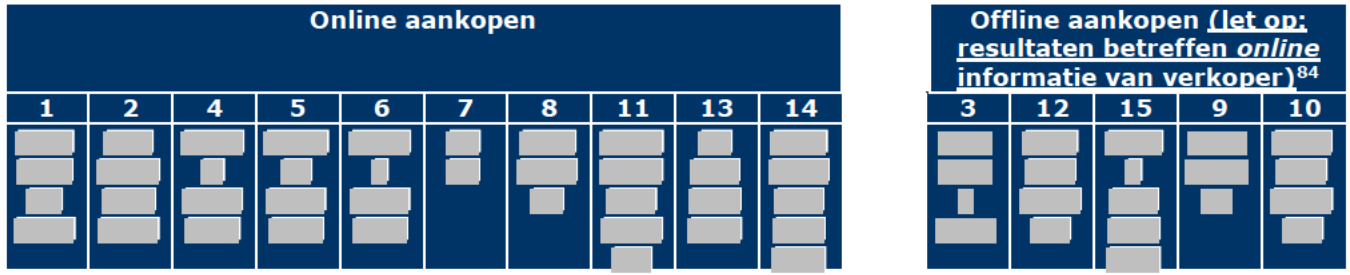
[82] Zie over deze 'dubbele uitdrukkelijkheidstoets' nader par. 2.1.

*Tabel 5 Overzicht gevonden online precontractueel verstrekte informatie door **verkoper***

	Online aankopen										Offline aankopen (let op: resultaten betreffen *online* informatie van verkoper)[83]				
	1	2	4	5	6	7	8	11	13	14	3	12	15	9	10
Informatie over functionaliteit, compatibiliteit en interoperabiliteit, updatebeleid precontractueel verstrekt door verkoper															
1. Minimumversie Android (smartphone) van bijbehorende app	Ja	Ja	Nee	Nee	Nee	n.v.t.	n.v.t.	Nee	Nee	Nee	Nee	Nee	Nee	n.v.t.	Nee
2. Minimumversie iOS/iPadOS van bijbehorende app	Ja	Ja	Nee	Nee	Nee	n.v.t.	n.v.t.	Nee	Nee	Nee	Nee	Nee	Nee	n.v.t.	Nee
3. Ondersteunde Wi-Fi-technologieën	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Ja	Nee	Nee	Nee
4. Ondersteunde Wi-Fi-frequenties	Ja	Ja	Ja	Ja	Ja	Ja	Nee	Nee	Ja	Ja	Nee	Ja	Nee	Nee	Nee
5. Gegarandeerde termijn voor volledige updates	Nee	Ja	Ja	Nee	Ja	Ja	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee
6. Gegarandeerde termijn voor beveiligingsupdates	Nee	Ja	Nee	Nee	Ja	Ja	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee
7. Ondersteunde smarthome-platformen, spraakassistenten	Ja	Ja	Nee	Nee	Nee	Nee	Ja	Ja	Nee	Nee	Ja	Ja	Nee	Nee	Ja
8. Ondersteunde opslagmedia	Nee	Nee	Ja	Ja	Ja	Nee	Nee	Nee	Nee	Nee	n.v.t.	n.v.t.	n.v.t.	Nee	n.v.t.
9. Ondersteunde Wi-Fi-beveiligingsmethoden	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Ja	Nee	Nee	Nee
10. Ondersteunde bedrade interfaces	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Ja	Ja	Ja	n.v.t.	n.v.t.	n.v.t.	Ja	n.v.t.	Ja	n.v.t.
11. Clouddienst nodig voor functies	Nee	Nee	Ja	Ja	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Ja
12. Internet nodig voor functies	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nee	Ja	Ja	Nee	Ja	Nee	Nee	Ja
13. Compatibele ZigBee-versie(s)	Ja	Ja	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Nee	n.v.t.	n.v.t.	n.v.t.	n.v.t.
14. Compatibele Thread-versie(s)	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
15. Compatibele 6LoWPAN-versie(s)	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Nee
16. Ondersteunt automatisch installeren van updates	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee
Aantal attributen verstrekt (van 16)	9	11	9	8	9	10	8	5	6	6	5	10	5	6	7

[83] Zoals eerder opgemerkt geven de resultaten die betrekking hebben op de apparaten die in dit onderzoek in een fysieke winkel zijn gekocht, geen inzicht in of er wordt voldaan aan de verplichtingen op het gebied precontractuele informatieverstrekking binnen de verkoopruimte.

*Tabel 6 Overzicht gevonden online precontractueel verstrekte informatie door **fabrikant***



	Online aankopen										Offline aankopen (let op: resultaten betreffen *online* informatie van verkoper)[84]				
	1	2	4	5	6	7	8	11	13	14	3	12	15	9	10
Informatie over functionaliteit, compatibiliteit en interoperabiliteit, updatebeleid precontractueel verstrekt door fabrikant															
1. Minimumversie Android (smartphone) van bijbehorende app	Ja	Ja	Ja	Ja	Ja	n.v.t.	n.v.t.	Nee	Ja	Nee	Ja	Ja	Ja	n.v.t.	Nee
2. Minimumversie iOS/iPadOS van bijbehorende app	Ja	Ja	Ja	Ja	Ja	n.v.t.	n.v.t.	Ja	Ja	Ja	Ja	Ja	Ja	n.v.t.	Ja
3. Ondersteunde Wi-Fi-technologieën	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Ja	Nee	Nee	Nee
4. Ondersteunde Wi-Fi-frequenties	Nee	Ja	Nee	Nee	Ja	Nee	Nee	Nee	Nee	Ja	Nee	Ja	Nee	Nee	Nee
5. Gegarandeerde termijn voor volledige updates	Nee	Ja	Nee	Nee	Ja	Nee	Ja	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee
6. Gegarandeerde termijn voor beveiligingsupdates	Nee	Ja	Nee	Nee	Ja	Nee	Ja	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee
7. Ondersteunde smarthome-platformen, spraakassistenten	Ja	Ja	Ja	Nee	Nee	Ja	Nee	Ja	Nee	Ja	Ja	Ja	Ja	Nee	Ja
8. Ondersteunde opslagmedia	Nee	Nee	Nee	Nee	Ja	Nee	Nee	Nee	Nee	Nee	n.v.t.	n.v.t.	n.v.t.	Nee	n.v.t.
9. Ondersteunde Wi-Fi-beveiligingsmethoden	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee
10. Ondersteunde bedrade interfaces	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Ja	Ja	Ja	n.v.t.	n.v.t.	n.v.t.	Ja	n.v.t.	Nee	n.v.t.
11. Clouddienst nodig voor functies	Nee	Nee	Ja	Ja	Ja	Nee	Nee	Nee	Nee	Ja	Nee	Nee	Nee	Nee	Nee
12. Internet nodig voor functies	Ja	Ja	Nee	Nee	Ja	Ja	Ja	Nee	Ja	Ja	Ja	Ja	Nee	Nee	Nee
13. Compatibele ZigBee-versie(s)	Ja	Ja	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Nee	n.v.t.	n.v.t.	n.v.t.	n.v.t.
14. Compatibele Thread-versie(s)	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
15. Compatibele 6LoWPAN-versie(s)	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Ja
16. Ondersteunt automatisch installeren van updates	Nee	Ja	Nee	Nee	Nee	Nee	Ja	Nee	Nee	Nee	Ja	Ja	Nee	Nee	Nee
Aantal attributen verstrekt (van 16)	**8**	**12**	**8**	**7**	**12**	**8**	**10**	**6**	**7**	**9**	**9**	**12**	**8**	**5**	**7**

[84] Zoals eerder opgemerkt geven de resultaten die betrekking hebben op de apparaten die in dit onderzoek in een fysieke winkel zijn gekocht, geen inzicht in of er wordt voldaan aan de verplichtingen op het gebied precontractuele informatieverstrekking binnen de verkoopruimte.

Tabel 7 Algemene voorwaarden verkoper en eindgebruikersovereenkomsten bij ingebruikname

Apparaat ID	Korte naam apparaat	Gebruiksvoorwaarden in app (c.q.op apparaat) accepteren noodzakelijk voor volledig gebruik	Gebruiksvoorwaarden gepresenteerd op productpagina verkoper	Gebruiksvoorwaarden gepresenteerd op productpagina fabrikant
1	[redacted]	Ja	Nee	Nee
2	[redacted]	Ja	Nee	Ja
3	[redacted]	Ja	Nee	Ja
4	[redacted]	Ja	Nee	n.v.t.
5	[redacted]	Nee	n.v.t.	n.v.t.
6	[redacted]	Ja	Nee	Nee
7	[redacted]	Ja	Nee	Nee
8	[redacted]	Ja	Nee	Nee
9	[redacted]	Ja	Nee	Nee
10	[redacted]	Ja	Nee	Ja
11	[redacted]	Ja	Nee	Nee, maar staat wel elders op de website (via Google te vinden)
12	[redacted]	Ja	Nee	Ja
13	[redacted]	Ja	Nee	Nee, maar staat wel elders op de website (via Google te vinden)
14	[redacted]	Ja	Nee	Op de website staat een ander document: 'Algemene voorwaarden [redacted]'
15	[redacted]	Ja	Nee	Nee

[redacted]

Vereist accepteren van gebruiksvoorwaarden

In Tabel 7 is voor elk product te zien of er algemene voorwaarden geaccepteerd moesten worden om het product volledig te kunnen gebruiken. Dit type algemene voorwaarden, waarvoor partijen verschillende namen kunnen hanteren, noemen we hier de *gebruiksvoorwaarden*. Ook is in de tabel te zien of die gebruiksvoorwaarden waren aangeboden op de productpagina van de verkoper en of zij waren aangeboden op de productpagina van de fabrikant. Merk op dat vrijwel elke fabrikant[85] (en verkoper) wel algemene voorwaarden op de website heeft staan, maar dat dit meestal niet de gebruiksvoorwaarden zijn die in de app of tv geaccepteerd moeten worden om het product (volledig) te kunnen gebruiken. Een consument die op de productpagina van de fabrikant 'de' algemene voorwaarden van de fabrikant vindt, wordt bij ingebruikname van het product dus vaak alsnog geconfronteerd met voorwaarden die hij niet eerder heeft ingezien.

Voor geen enkel van de onderzochte apparaten stonden de gebruiksvoorwaarden op de website van de verkoper[86], noch informeert de verkoper op de productpagina over het feit dat het nodig is akkoord te gaan met een dergelijke voorwaarden bij ingebruikname. De gebruiksvoorwaarden waren ook lang niet altijd te vinden op de website van de fabrikant zelf.

Juridische duiding

Als de consument feitelijk gedwongen is de toepasselijkheid van algemene voorwaarden *alsnog* te aanvaarden bij het installeren van het domotica-apparaat om dat volledig te kunnen gebruiken, is de overeenkomst met de fabrikant vernietigbaar wegens misbruik van omstandigheden (art. 3:44 lid 1 jo. lid 4 BW) dan wel een agressieve handelspraktijk (art. 6:193h lid 1 jo. 193j lid 3 BW), nu de consument feitelijk wordt gedwongen akkoord te gaan met het sluiten van een overeenkomst om het domotica-apparaat te kunnen gebruiken dat hij al gekocht heeft, terwijl de fabrikant geen recht kan doen gelden op de toepassing van de licentievoorwaarden. Ook de koopovereenkomst met de verkoper kan, in dat geval wegens een misleidende omissie (art. 6:193d lid 2 jo. 193f onder b jo. 193j lid 3 BW) worden vernietigd; zie in dit verband nader par. 2.1.

Inhoud van de gebruiksvoorwaarden

Tabel 8 toont per apparaat welke relevante elementen (op gebied van functionaliteit, compatibiliteit en interoperabiliteit en updatebeleid) werden aangetroffen in de gebruiksvoorwaarden per apparaat.

Veelal bevatten de te accepteren voorwaarden geen bepalingen over FCIU, maar enkel over zaken als garantie, aansprakelijkheid, herroepingsrecht, et cetera. Omdat vaak dezelfde gebruiksvoorwaarden voor meerdere apparaten worden gehanteerd, bevatten zij eigenlijk nooit informatie over de functionaliteit of compatibiliteit van het specifieke apparaat. Hieronder bespreken we kort enkele bevindingen, in de tabel is aangegeven bij welke apparaten we welke informatie zijn tegengekomen. Voor de app bij de [redacted] babyfoon ([redacted]) hoefde geen voorwaarden geaccepteerd te worden.

De gevonden bepalingen over **interoperabiliteit** houden in dat het bedrijf ([redacted]) niet garandeert dat het product werkt met apparaten van derden die niet door het bedrijf zijn aangewezen, zelfs als deze apparaten hetzelfde protocol

[85] Van de [redacted] en [redacted] babyfoons is de fabrikant onbekend en is dus geen website beschikbaar waar de gebruiksvoorwaarden op gepresenteerd zouden kunnen worden.

[86] Op basis van de informatie die is verzameld volgens de gehanteerde testmethode.

gebruiken. [redacted]. Met betrekking tot **functionaliteit** geeft [redacted] aan dat de functionaliteit per apparaat verschilt en dat alleen van de volledige functionaliteit van de app gebruik kan worden gemaakt als de gebruiker in de app is ingelogd. Verder komen FCIU-kenmerken enkel terug in het kader van **updates**. Soms wordt namelijk gesteld dat updates kunnen leiden tot het wijzigen of verdwijnen van functies.

Sommige partijen gaan daarnaast in op de wijze van installeren van updates (automatisch, geforceerd of handmatig), het belang of de mogelijke doelen van updates (bug-fixes, veiligheid, uitbreiding functionaliteit) of het feit dat sommige updates verplicht zijn of automatisch geïnstalleerd worden ongeacht de instellingen van de gebruiker (bijvoorbeeld in het geval van kritieke veiligheidsupdates). Het niet installeren van bepaalde updates kan volgens sommige voorwaarden leiden tot een beperking van aansprakelijkheid van de fabrikant, of tot het onbruikbaar worden van het apparaat. Het toetsen van de voorwaarden valt buiten de scope van dit onderzoek. In Tabel 8 geven we enkel aan welke onderwerpen we in de gebruiksvoorwaarden bij de apparaten zijn tegengekomen. Voor de vereisten omtrent informatieverstrekking verwijzen we naar paragraaf 2.1.

Tabel 8 Overzicht inhoud gebruiksvoorwaarden per apparaat

Apparaat ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Apparaat															
Functionaliteit	Nee	Nee	Nee	Nee	n.v.t.	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Ja
Compatibiliteit	Nee	Nee	Nee	Nee	n.v.t.	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee
Interoperabiliteit	Nee	Ja	Ja	Nee	n.v.t.	Nee	Nee	Nee	Nee	Nee	Nee	Ja	Nee	Ja	Nee
Updates kunnen leiden tot verminderde FCI	Nee	Ja	Nee	Nee	n.v.t.	Nee	Ja	Nee	Ja	Nee	Ja	Nee	Ja	Ja	Nee
Wijze van installeren updates	Nee	Ja	Ja	Nee	n.v.t.	Nee	Nee	Nee	Nee	Nee	Nee	Ja	Nee	Ja	Ja
Belang van updates	Nee	Ja	Ja	Nee	n.v.t.	Nee	Nee	Nee	Nee	Nee	Nee	Ja	Ja	Ja	Ja
Niet installeren updates kan aanspra-kelijkheid beperken	Nee	Nee	Ja	Nee	n.v.t.	Nee	Nee	Nee	Nee	Nee	Nee	Ja	Nee	Nee	Nee
Sommige updates zijn verplicht (apparaat anders onbruikbaar)	Nee	Nee	Ja	Nee	n.v.t.	Nee	Ja	Nee	Ja	Nee	Ja	Ja	Ja	Ja	Ja
Updatetermijn	Nee	Ja	Nee	Nee	n.v.t.	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Ja

White label-apparaten

Voor een klein aantal ('white label') apparaten is niet goed vast te stellen *wie* de fabrikant is. Waar bij andere apparaten de website van de fabrikant veel detailinformatie kan geven in de precontractuele fase (denk aan technische specificaties, handleidingen, juridische kennisgevingen), wat overigens niet afdoet aan de informatieverplichtingen van de verkoper, is de consument voor informatie over de 'white label'- apparaten vrijwel volledig aangewezen op de verkoper. De enige interactie tussen consument en (indirect) de fabrikant is het installeren en gebruiken van de app (die door de fabrikant wordt aangeboden in de app stores).

4.3 Ingebruiknamefase

De apparaten zijn tussen 22 maart 2022 en 31 maart 2022 in gebruik genomen. Op het eerste ingebruiknamemoment (22 maart 2022) zijn alle apparaten allereerst fysiek geïnstalleerd. Vervolgens is een eerste poging gedaan om, volgens de instructies uit de handleiding/de verpakking, het product te installeren.

Vanaf het eerste ingebruiknamemoment was op het testnetwerk TLS-interceptie actief. Doel hiervan was om te bepalen of en zo ja hoe apparaten communiceerden met het internet en daarbij 'afluisteren' van TLS-verkeer zouden accepteren. Bij veruit de meeste apparaten leidde de TLS-interceptie er echter toe dat de ingebruikname niet (volledig) kon worden voltooid (een niet onverwacht en op zich positief resultaat). Daarnaast leidde segmentering van het vaste en het draadloze netwerk ertoe dat in sommige gevallen apps het bijbehorende bedraad aangesloten apparaat (m.n. de domotica-hubs) niet konden 'vinden'. De segmentering was aangebracht om verkeer tussen applicatie en de gekoppelde apparaten te kunnen monitoren.

De testopstelling is vervolgens aangepast, zodat de apparaten vrijelijk ('zoals thuis') met het internet kunnen communiceren. Daarnaast is een aanpassing gedaan zodat het verkeer tussen applicatie en apparaat kan worden gemonitord, maar de verbinding daartussen niet in de weg staat.[87]

Op 31 maart waren alle apparaten voor het eerst allen volledig 'in gebruik'.

4.3.1 Toewijzing naar gebruikersapparaten

Bij het in gebruik nemen van de apparaten zijn de instructies van de fabrikant uit (primair) de bijgeleverde handleiding en/of op de verpakking gevolgd. Wanneer deze instructies aangaven dat er een app diende te worden gebruikt (om 'smart' functionaliteit te kunnen gebruiken), hebben wij deze geïnstalleerd uit de Apple App Store resp. Google Play Store. Zoals beschreven in de methodologie wijzen we de apparaten toe aan ofwel het iOS- ofwel het Android-gebruikersapparaat. Onderstaande Tabel 9 toont de apparaten waarvoor een app werd gebruikt in de test en op welk platform deze applicatie was geïnstalleerd.

[87] Specifiek: voor de gebruikte Android- en iOS-devices is een separaat Wi-Fi-netwerk opgezet. Verkeer tussen dit netwerk en het (vaste en bedrade) netwerk waarop de apparaten zijn aangesloten kan zo worden gemonitord. Wanneer dit nodig is (bijvoorbeeld als een app een product niet kan detecteren op het netwerk) kan op de devices worden overgeschakeld naar het netwerk van de apparaten. Dit verkeer kan dan niet meer worden gemonitord, omdat dit binnen hetzelfde ethernetsegment blijft en daarom op laag-2 (switch)-niveau wordt afgewikkeld. Verkeer van en naar het internet is te allen tijde gemonitord.

Tabel 9 Overzicht apps en platforms die onderdeel uitmaakten van de test

ID	Korte productnaam	Platform voor app	Naam app
1		iOS	
2		iOS	
3		Android	
4		iOS	
5		Android	
6		Android	
7		Android	
8		iOS	
9		Android	
10		Android	
11		iOS	
12		iOS	
13		Android	
14		iOS	
15		iOS	

Als iOS-apparaat is een (volledig geschoonde) iPad Air 2 (model MNV22HC/A) uit 2017 gebruikt met iOS 15.0 (19A346). Er is bewust voor gekozen om een tablet te gebruiken met een iets oudere versie van iOS (ten behoeve van het testen van compatibiliteit). Hierbij zijn geen problemen opgetreden; alle apps bleken compatibel met de gebruikte iPad en er is geen beperking van functionaliteit geconstateerd. Als Android-apparaat is een Motorola Moto G 20-smartphone gebruikt. Gedurende de test kwam een update voor het Android-besturingssysteem voor deze telefoon beschikbaar; deze is geïnstalleerd. Overige details over de gebruikersapparaten zijn te vinden in Bijlage 5.

Gedurende de ingebruikname zijn alle apparaten aangesloten op het testnetwerk. Voor de meeste apparaten geldt dat zij zijn aangesloten op een draadloos netwerk. De apparaten 1, 2 en 10 zijn bedraad aangesloten. De slimme televisies (7, 8, 9) konden zowel draadloos als bedraad worden aangesloten. Deze apparaten zijn draadloos aangesloten (overigens is wel vastgesteld dat de bedrade aansluiting functioneerde).

4.3.2 Functionaliteit

Er zijn geen substantiële afwijkingen gevonden tussen de door de verkoper noch de fabrikant gespecificeerde informatie over functionaliteit en de feitelijke functionaliteit van de apparatuur.

Voor vrijwel alle apparaten was het accepteren van bepaalde algemene voorwaarden van de fabrikant vereist om alle functies (met name de functies die gebruik maken van onlinediensten van de fabrikant, waaronder ook updates) te kunnen gebruiken. Op één uitzondering na vereiste elke app dat akkoord werd gegaan met gebruiksvoorwaarden. Ook bij de tv's, waar geen sprake was van een losse app, moesten gebruiksvoorwaarden geaccepteerd worden om de tv volledig te kunnen gebruiken.

4.3.3 Compatibiliteit en interoperabiliteit

Alle apparaten waren compatibel met de testopstelling en daarin gebruikte apparaten bij ingebruikname. Dit is positief, gegeven het feit dat de testopstelling lijkt op een 'standaard' consumentenomgeving (voor wat betreft internet en Wi-Fi).

Verificatie van de precontractuele informatie over compatibiliteit met de feitelijke situatie is voor veel apparaten lastig of onmogelijk, omdat de verkoper vaak alleen specificeert dát een apparaat compatibel is met een bepaald platform, besturingssysteem of bijvoorbeeld draadloze connectiviteit, maar daarbij geen concrete versienummers zijn aangegeven. Deze versienummers zijn (voor de bijbehorende apps) wel terug te vinden in de betreffende app store.

Bij offline aankopen was de verstrekte informatie over compatibiliteit met bepaalde app-platforms beperkter of minder precies (bijvoorbeeld: "werkt met Apple-telefoons" zonder specificatie van een exacte iOS-versie).

Juridische duiding

Op basis van de informatieplicht van art. 6:230l onder h en 230m lid 1 onder s BW moet de verkoper in ieder geval informatie verstrekken over de minimaal vereiste systeemversie van de besturingssoftware en de versie van de software die het domotica-apparaat zelf gebruikt. Gebeurt dit niet, dan is de overeenkomst vernietigbaar op grond van art. 6:193d jo. 193j lid 3 BW (zie par. 2.1).

Het koppelen met Wi-Fi-netwerken blijkt bij de wasmachines in het algemeen (o.a. vanwege de beperkte interface op het apparaat en de koppelmethode) vaker te mislukken om onduidelijke redenen. Uiteindelijk zijn alle wasmachines (simpelweg door de procedure een aantal keer te herhalen) met succes verbonden aan het testnetwerk.

Alle apparaten interopereren naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is (dan zouden we immers alle mogelijke interoperabele apparaten en diensten moeten testen) zijn er geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.

Verificatie van de precontractuele informatie over specifieke interoperabiliteit met de feitelijke situatie is voor veel apparaten niet eenduidig te doen, omdat de verkoper/fabrikant vaak alleen specificeert dát een apparaat kan werken met een bepaald platform, en daarbij geen specifieke apparaten of versienummers noemt.

4.3.4 Updatebeleid

Bij een aantal apparaten was precontractueel geen (volledige) informatie beschikbaar over het updatebeleid. Vaak is alleen aangegeven dat het product updates kan accepteren, en niet of er updates zullen worden uitgebracht, met welke frequentie, noch met welke inhoud (functionaliteit of alleen beveiligingsupdates), en of het updaten automatisch kan worden uitgevoerd door de app en/of het apparaat zelf.

Voor geen van de apparaten vonden we een verschil in termijn voor 'volledige' versus 'beperkte' updates. Aangenomen moet dan ook worden dat de termijn die wordt genoemd verwijst naar updates zoals beschreven in regelgeving (kort gezegd: minimaal de updates die nodig zijn om het product conform te houden).

4.3.5 Digitale veiligheid

Direct na de ingebruikname is een analyse uitgevoerd van de digitale veiligheid. De resultaten hiervan zijn te vinden in de testmatrix (Bijlage 4). Tegen het einde van de testperiode is een tweede analyse van digitale veiligheid uitgevoerd. De uitkomsten ten aanzien van overeenstemming met de onderzochte vereisten op het gebied van digitale veiligheid verschillen nauwelijks tussen beide meetmomenten. We volstaan daarom in dit rapport met de beschrijving van de resultaten van de tweede analyse (waarbij we ingaan op de verschillen ten opzichte van de eerste meting). De resultaten van beide meetmomenten zijn per apparaat terug te vinden in Bijlage 4.

4.4 Gebruiksfase

In deze paragraaf geven we de resultaten van de analyses die zijn uitgevoerd gedurende de gebruiksperiode op het gebied van functionaliteit, compatibiliteit, interoperabiliteit, updatebeleid en digitale veiligheid.

We beperken ons hier tot de bevindingen op hoofdlijnen voor de steekproef als geheel. Zoals beschreven in de methodiek zijn gedurende de testperiode op meerdere momenten analyses uitgevoerd. Gedetailleerde resultaten per apparaat in de steekproef en per moment zijn te vinden in Bijlage 3.

4.4.1 Functionaliteit, compatibiliteit en interoperabiliteit

Gedurende de testperiode zijn er 22 updates beschikbaar gekomen voor de apparaatsoftware van acht apparaten. De updategeschiedenis en de resultaten van de checks per apparaat zijn te vinden in Bijlage 3 (Tabel 13).

- **Geen van de gedurende de ingebruikname en testperiode aangeboden updates van de apparaatsoftware heeft geleid tot een voor de onderzoekers zichtbare wijziging van functionaliteit, compatibiliteit en interoperabiliteit**.[88]

- **De minimumversie van het besturingssysteem waarop de bij een apparaat behorende app werkt, is voor acht (van de twaalf apparaten die met app getest zijn) gedurende de testperiode verhoogd.**

  Met 'verhogen van de minimumversie' bedoelen we dat de minimumversie van het besturingssysteem die nodig is om een update van de app te installeren, hoger is dan voor de vorige versie van de app.[89] Wanneer het besturingssysteem op het gebruikersapparaat niet aan het minimum voldoet, betekent dit dat de update niet kan worden geïnstalleerd. Tenzij er wijzigingen aan zijde van de dienst van de fabrikant plaatsvinden leidt het verhogen van de minimumversie er overigens niet toe dat de 'oudere' app stopt met werken. Een reden om de minimumversie te verhogen kan zijn dat nieuwere versies van het besturingssysteem aanvullende apparaatfuncties beschikbaar maken voor apps, en de fabrikant deze functie wil gebruiken. Daarnaast

[88] Op basis van controle van de eerder gedefinieerd FCIU-kenmerken (zie Tabel 1). Zoals eerder opgemerkt is deze set kenmerken niet-uitputtend. Het is uiteraard denkbaar dat een update de compatibiliteit/interoperabiliteit met een specifiek stuk software of hardware beïnvloedt (bijvoorbeeld als de code een clausule bevat die alleen wordt geactiveerd wanneer wordt gekoppeld met een specifiek type ander apparaat). Het is praktisch gezien onmogelijk om compatibiliteit met álle mogelijke software of hardware te controleren.

[89] De minimaal vereiste versie van het besturingssysteem is in beginsel een eigenschap van de app en is te vinden in de metadata van het softwarepakket ('binary') zoals gedownload uit bijvoorbeeld een app store. De minimumversie wordt daarnaast weergegeven in de App Store van Apple.

worden ook de ontwikkelomgevingen waarin de fabrikanten werken bijgewerkt wanneer nieuwe versies van een besturingssysteem worden uitgebracht, waarbij ondersteuning voor oudere besturingssystemen eveneens kan komen te vervallen.

De wijzigingen van de minimumversies per apparaat zijn te vinden in Bijlage 3 (Tabel 11). De wijzigingen van de minimumversie van iOS in onze steekproef leiden voor zover bekend niet tot het uitsluiten van oudere apparaten die werken met iOS (de nieuwere minimaal vereiste iOS-versie werkt op alle modellen die ook de oudere versie ondersteunden). Bij de Android-apps is lastiger vast te stellen welk deel van de apparaten door de wijziging wordt uitgesloten. Over het algemeen gaat het overigens om een verhoging van de minimumversie naar een versie die al enige jaren geleden voor het eerst uitkwam (bijvoorbeeld van iOS 11 naar iOS 12, terwijl de actuele versie iOS 15 is, en er jaarlijks een nieuwe versie wordt uitgebracht).

Een verhoging van de minimumversie betekent dat gebruikers zijn aangewezen op de laatste versie van de app vóór de wijziging (en een risico dat er geen updates meer worden uitgebracht voor de app).

Juridische duiding

Bovenstaande kan betekenen dat de verkoper tekort schiet in zijn verplichting om updates te leveren, zoals deze verplichting voortvloeit uit art. 7:18 lid 4 BW. Of dat het geval is, hangt af van de vraag of de consument nog updates – in het bijzonder veiligheidsupdates – mocht verwachten.[90] Dat hangt in het bijzonder af van het moment waarop de consument het domotica-apparaat heeft *aangeschaft* en de informatie die hem toen is verstrekt over de duur van het beschikbaar zijn van updates: het is immers op basis van het moment van contractsluiting (en niet het moment waarop het domotica-apparaat op de markt is gebracht) hoe lang de consument redelijkerwijs nog updates mocht verwachten. Daarvan mag de verkoper echter wel afwijken ten nadele van de consument, mits daarbij aan de in par. 2.1 genoemde 'dubbele uitdrukkelijkheidstoets' is voldaan.

- **Wasmachines zijn lastig te koppelen aan een Wi-Fi-netwerk, en verliezen af en toe de verbinding.** Opvallend is dat één wasmachine in de steekproef (apparaat 14) voortdurend de verbinding met het Wi-Fi-netwerk verloor. Deze wasmachine hebben wij in deze gevallen enkele dagen de kans gegeven zelf de verbinding te herstellen, waarna de koppelprocedure opnieuw werd doorlopen (waarbij uiteraard werd gecontroleerd of er niet in de tussentijd een update beschikbaar is gekomen voor het apparaat). Het is ons niet duidelijk waarom deze wasmachine de verbinding steeds verliest, maar gezien onze ervaringen bij de ingebruikname lijkt het dat de kwaliteit van de implementatie van Wi-Fi bij specifiek wasmachines te wensen overlaat.

[90] Zie hierover ook overweging 31 Richtlijn (EU) 2019/771: *"Normaal gesproken zou een consument verwachten updates te ontvangen gedurende ten minste de periode gedurende welke de verkoper aansprakelijk is voor een conformiteitsgebrek, hoewel de redelijke verwachting van de consument in sommige gevallen langer is dan die periode, in het bijzonder in het geval van beveiligingsupdates."*

4.4.2 Updatebeleid

Van de 15 apparaten was voor 8 apparaten een update beschikbaar in de periode tussen ingebruikname en 20 april 2022 (merk hierbij op dat een aantal apparaten op 25 maart in gebruik is genomen en een aantal later, op 30 maart).

Van de 11 apparaten die met een iOS/Android-app worden getest, zijn 5 apps tussen 1 april en 20 april (automatisch) voorzien van een update.

- **Zeven van de 15 apparaten uit de steekproef hebben tijdens de testperiode geen enkele update ontvangen. Een aantal apparaten ontving alleen direct na ingebruikname een update.** Gezien de bevindingen op het vlak van digitale veiligheid zouden we voor een aantal apparaten ten minste een beveiligingsupdate verwachten. Het valt op dat de gebruikersapps regelmatiger worden bijgewerkt.

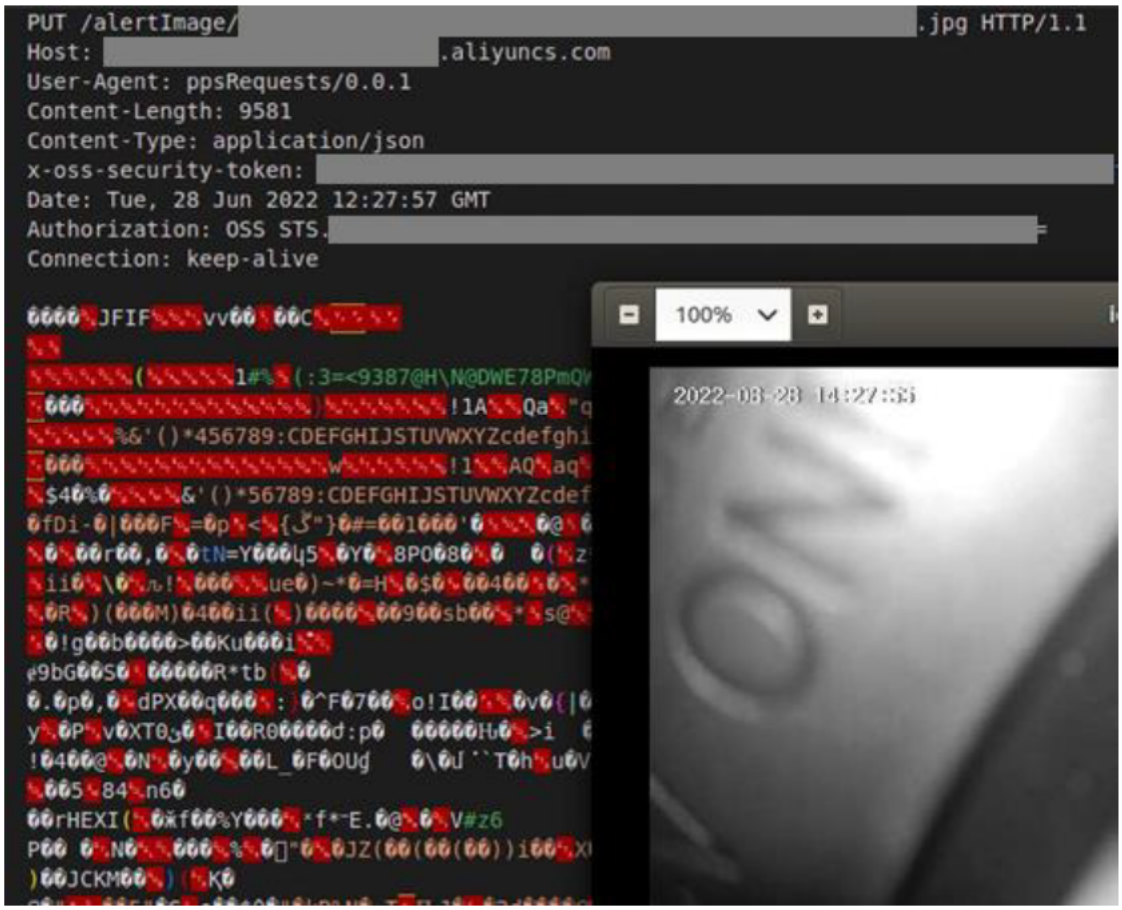
- **Wanneer een apparaat wordt gebruikt in combinatie met een compatibel basisstation zijn updates van het apparaat niet altijd mogelijk.** In de steekproef is een bundel van een slimme lamp in combinatie met een basisstation van een andere fabrikant meegenomen (apparaat 3). Hoewel de slimme lamp interoperabel bleek met dit basisstation, konden we het versienummer van de software op de lamp niet achterhalen via de bijbehorende app, en hebben we het sterke vermoeden dat dit basisstation niet in staat is om de software op de lamp bij te werken. In de steekproef testten we hetzelfde type lamp ook met het basisstation van de fabrikant van de lamp (apparaat 2), en de lamp ontving hier twee updates (kort na ingebruikname en tegen het einde van de testperiode).

- **Wij hebben vanaf het moment van aankoop tot het einde van de gebruiksperiode geen e-mailberichten en geen sms-berichten van verkopers noch fabrikanten ontvangen aangaande software-updates voor de online bestelde apparaten.** Bij online aankopen hebben we steeds een e-mailadres achtergelaten. Voor het aanmaken van accounts in de apps is een ander e-mailadres gebruikt. Wanneer een telefoonnummer werd gevraagd hebben we hiervoor een specifiek voor dit onderzoek geactiveerd nummer op basis van een mobiel sim-only abonnement gebruikt. Na afloop van de gebruiksperiode zijn beide mailboxen en de ontvangen sms-berichten geanalyseerd. Voor slechts één apparaat ontvingen we een melding van een update. Dit betrof een e-mail van de fabrikant. De update bestond uit het toevoegen van functionaliteit en een nieuwe abonnementsmogelijkheid in de app.

4.4.3 Digitale veiligheid

Het algemene beeld is dat de digitale veiligheid van de onderzochte apparaten op orde is, gegeven de criteria die in dit onderzoek centraal stonden. Deze criteria zien op 'best practices' alsmede de 'lokale' veiligheid van het apparaat (dat wil zeggen, jegens aanvallers die zich op het lokale netwerk bevinden waarop ook het apparaat is aangesloten). Op dit algemene positieve beeld zien we een aantal uitzonderingen:

- **Voor één product (nummer 5, babyfoon) constateerden we dat deze periodiek, onversleuteld en zonder toestemming van de gebruiker afbeeldingen, gemaakt met de camera, via internet verzond naar een server.** Onduidelijk is met welk doel deze afbeeldingen worden verzonden. Het is ons niet gelukt een mogelijkheid te vinden (in de app) om het verzenden van de beelden te stoppen. De fabrikant van deze babyfoon hebben wij (volgens de beschreven procedure voor *coordinated vulnerability disclosure*) hiervan op de hoogte gesteld. Figuur 11 toont hoe dit onversleutelde verkeer zichtbaar is voor een aanvaller (die zich bijvoorbeeld op hetzelfde lokale netwerk bevindt).



Figuur 11 Een babyfoon uit de steekproef verstuurt onversleuteld een afbeelding naar een server op internet

Privacy bij onlinediensten

Apparaten die afhankelijk zijn van een dienst van een fabrikant versturen persoonsgegevens (zoals, in het geval van babyfoons, camerabeelden) naar deze dienst. De aanbieder moet uiteraard de juiste maatregelen treffen om te voldoen aan de AVG (zoals beveiligingsmaatregelen, maar ook bijvoorbeeld het tijdig verwijderen van de gegevens). Het is 'van buitenaf' (voor een eindgebruiker en zelfs op basis van technische analyse zoals in dit onderzoek) niet goed vast te stellen of een aanbieder dit inderdaad op orde heeft.

Een technische oplossing om het risico op lekken of misbruik van persoonsgegevens te beperken, is *end to end-encryptie*. Hierbij worden gegevens voordat ze naar de dienst worden verzonden versleuteld met een sleutel waarover alleen de gebruiker beschikt. De dienst fungeert hierbij alleen als 'doorgeefluik': ze slaat de gegevens op, maar kan ze niet ontsleutelen. Uiteraard is hierbij van belang dat een sterke sleutel wordt gebruikt, dat de uitwisseling van deze sleutel (tussen het apparaat en het gebruikersapparaat) veilig verloopt, en dat er geen mogelijkheid is om de sleutel te ontfutselen van het apparaat en het gebruikersapparaat.

- **Een aantal** apparaten **past een verouderde, onveilige versie van het STUN-protocol toe.** STUN (*Session Traversal Utilities for NAT)* is een protocol waarmee een apparaat binnen het netwerk van een thuisgebruiker van buitenaf bereikbaar kan worden gemaakt. Dit is nodig wanneer het apparaat zich bijvoorbeeld achter een

thuisrouter bevindt die alleen uitgaande verbindingen toestaat, en waarbij meerdere apparaten op het netwerk hetzelfde publieke IP-adres delen. Het gebruik van STUN op zichzelf is geen veiligheidsrisico. We constateren echter dat een aantal apparaten STUN op een onveilige manier gebruikt. De onveiligheid bestaat eruit dat de STUN-verbinding wordt opgezet op basis van een sleutel die te achterhalen is voor iemand die het STUN-verkeer kan afluisteren. Hiermee zou een aanvaller (afhankelijk van de verdere configuratie en kennis over de dienst) oneigenlijke toegang kunnen krijgen tot delen van de dienst van de fabrikant. Gezien de scope van dit onderzoek is dit niet verder uitgediept.

Merk bij bovenstaande op dat het een kwetsbaarheid in de *dienst van de fabrikant* betreft en, technisch gezien, niet in het apparaat zelf. Het ontbreken van de dienst zou er echter toe kunnen[91] leiden dat het apparaat een deel van zijn functies niet kan vervullen (dat maakt het een 'zaak met digitale elementen', zie paragraaf 2.1). De apparaten die via een verouderde versie van het STUN-protocol contact leggen met die dienst zullen moeten worden voorzien van een update om het oplossen van de zwakheid in de dienst mogelijk te maken.

- **Een aantal 'best practices' voor het beveiligen van verbindingen wordt niet opgevolgd.** Het protocol dat meestal wordt gebruikt voor beveiliging van verbindingen (TLS) is veilig, maar moet dan wel juist worden geïmplementeerd. De aanbevelingen hiervoor zijn, als gevolg van het ontdekken van veiligheidsrisico's in TLS en de bijbehorende 'ciphers' (versleutelingsalgoritmes waarvan TLS gebruik kan maken) aan verandering onderhevig. Fabrikanten moeten het gebruik van TLS dan ook continu bijwerken naargelang de laatste 'best practices'. In de steekproef vinden we enkele apparaten waarvoor dit niet het geval is.

- **Een babyfoon staat de gebruiker toe om onveilige toegang tot camerabeelden te activeren**. Via het gestandaardiseerde ONVIF-protocol kunnen beelden van een babyfoon worden uitgelezen door andere applicaties dan die van de fabrikant. Het protocol staat standaard uitgeschakeld. Na inschakelen blijkt voor één babyfoon (apparaat 5) dat toegang mogelijk is met een zeer eenvoudig wachtwoord ('0000'), ook nog eens over een niet-beveiligde verbinding. Het wachtwoord is weliswaar te wijzigen (deze mogelijkheid bevindt zich op dezelfde instellingenpagina), maar daarbij worden geen complexiteitseisen gehandhaafd. Figuur 12 laat zien hoe dit in zijn werk gaat. De inloggegevens worden weliswaar 'gecodeerd', maar de codering is niet veel meer dan een andere notatie (Base64) die eenvoudig kan worden teruggedraaid.

[91] Dit is afhankelijk van de configuratie van het netwerk en de internetaansluiting van de gebruiker. Deze bepaalt of de STUN-dienst nodig is.

Figuur 12 Poging om verbinding te maken met de ONVIF-ingang van een babyfoon met eenvoudige gebruikersnaam en wachtwoord

- **Diverse apparaten geven informatie over de software (zoals versienummers) prijs.** Op zichzelf zou het bekend worden van de specifieke software en -versienummers daarvan die op een apparaat worden gebruikt niet direct moeten leiden tot een zwakheid. Desondanks kunnen aanvallers de informatie gebruiken om zwakheden op te zoeken in databases, en daardoor sneller te werk gaan. Een 'best practice' voor IoT-apparaten is dan ook om software- en versie-informatie zoveel mogelijk te verbergen. Voor een aantal apparaten in de steekproef is de informatie echter relatief eenvoudig te verkrijgen.

Afhankelijkheid van en communicatie met een onlinedienst

De eerste generatie slimme apparaten maakte veelal gebruik van rechtstreekse communicatie met het eindgebruikersapparaat over het lokale netwerk van de gebruiker. In sommige gevallen werd zelfs gebruik gemaakt van een webinterface. Deze apparaten zijn zonder internetverbinding te gebruiken. Het nadeel is dat de communicatie tussen apparaat en gebruikersapparaat vaak niet (goed) versleuteld is en de veiligheid sterk afhankelijk is van de veiligheid van het netwerk van de gebruiker. Omdat de apparaten niet per definitie met internet hoefden te communiceren gold voor veel apparaten dat het bijwerken van de software niet automatisch plaatsvond (als dit al mogelijk was).

De onderzochte apparaten zijn duidelijk van een nieuwere generatie. Vrijwel alle apparaten maken gebruik van communicatie via een dienst van de fabrikant (hiernaar wordt vaak verwezen als 'de cloud'). De communicatie met de clouddienst verloopt uiteraard over het netwerk van de gebruiker, maar deze communicatie is over het algemeen goed beveiligd, doordat gebruik kan worden gemaakt van de standaarden die hiervoor algemeen op het internet worden gebruikt (TLS met certificaten).

Directe communicatie tussen gebruikersapparaten en het IoT-apparaat vindt nauwelijks meer plaats – bij de meeste apparaten alleen nog om deze met elkaar te koppelen

(zodat de clouddienst weet dat een IoT-apparaat met serienummer X hoort bij gebruikersaccount Y).[92]

De beperktere communicatie op het lokale netwerk leidt tot een kleine(re) 'attack surface' voor deze apparaten vanuit het perspectief van een aanvaller met netwerktoegang tot het apparaat. Hoewel de communicatie met de onlinediensten over het algemeen veilig lijkt te verlopen, betekent de vereiste om een clouddienst te gebruiken wel dat de veiligheid van deze clouddienst (die in dit onderzoek buiten scope valt) van groot belang is. De veiligheid van de clouddiensten is in dit onderzoek niet getoetst. Het is daarnaast van buitenaf lastig te bepalen of een clouddienst veilig is geïmplementeerd (en of dit ook is geborgd). Een tweede nadeel van de afhankelijkheid van clouddiensten is dat de apparaten mogelijk niet meer (volledig) functioneren wanneer de clouddienst niet bereikbaar is (bijvoorbeeld als de internetverbinding of de clouddienst is uitgevallen, of wanneer de fabrikant heeft besloten de clouddienst stop te zetten).

Onderstaande Tabel 10 toont de resultaten voor alle onderzochte vereisten, uitgesplitst naar resultaat. In de tabel worden alleen de vereisten getoond waarop ten minste één afwijking (voldoet niet, of voldoet met waarschuwing) is geconstateerd. De cijfers betreffen het aantal apparaten. De cijfers in de blauwe (totaal)regels betreffen het aantal tests en zijn inclusief de niet-getoonde vereisten (waarvoor geen uitzonderingen werden gevonden). In sommige gevallen was een vereiste niet van toepassing – in de onderstaande tabel is dit geteld als "voldoet". In andere gevallen kon een vereiste (door beperkingen in de testopzet of om andere technische reden) niet getest worden. In dat geval telt het totaal van een rij niet op tot het aantal apparaten in de steekproef (15).

[92] De precieze implementatie verschilt per apparaat. Een mogelijke invulling is de volgende: (1) De gebruiker maakt een account voor de clouddienst van de fabrikant en logt daarmee in (beide vinden plaats in de app). (2) Het apparaat wordt in een 'koppelingsmodus' gezet (of staat dit bij eerste ingebruikname). Het apparaat rapporteert het eigen serienummer aan de clouddienst. (2) De applicatie zoekt via specifiek daarvoor bestemde netwerkprotocollen of een apparaat van een bepaald type in het lokale netwerk te vinden is (omdat het apparaat in koppelingsmodus staat is deze vindbaar). (2) De applicatie vraagt het serienummer van dit apparaat op en/of communiceert via het lokale netwerk met het apparaat om een digitaal 'bewijs' te creëren dat het apparaat zich binnen hetzelfde netwerk bevindt als de applicatie. (4) De app verstuurt het serienummer en/of het digitale bewijs naar de clouddienst. (5) De clouddienst voegt het apparaat op basis van serienummer toe aan het account waarmee de gebruiker is ingelogd in de app.

Tabel 10 Uitkomsten tests digitale veiligheid naar resultaat per vereiste (alleen voor de vereisten met geconstateerde afwijkingen worden details getoond – de totalen betreffen alle geteste vereisten)

		Oordeel		
Vereiste	**Beschrijving (Engelstalige beschrijving van de vereiste uit het gehanteerde raamwerk)**	**Voldoet niet**	**Voldoet met waarschuwing**	**Voldoet of n.v.t.**
Qbit 4.7.1	**All passwords must conform to the industry standard NIST SP800-63b Digital Identity Guidelines.**	**3**	**0**	**177**
IoTSF 2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.	**1**	0	14
IoTSF 2.4.8.6	Password entry follows industry standard practice on password length, characters from the groupings and special characters.	**1**	0	14
IoTSF 2.4.8.7	The product has defence against brute force repeated login attempts, such as exponentially increasing retry attempt delays.	**1**	0	14
Qbit 4.7.2	**Access to device functionality via a network interface in the initialised state must only be possible after authentication on that interface.**	**0**	**0**	**90**
Qbit 4.7.3	**All exposed ports and interfaces must be necessary for the normal and intended use of the device.**	**0**	**0**	**15**
Qbit 4.7.4	**All network traffic must be encrypted and authenticated using best practice encryption protocols, such as TLS.**	**9**	**0**	**211**
IoTSF 2.4.7.13	Where a TCP protocol, such as MQTT, is used, it is protected by a TLS connection with no known vulnerabilities.	**2**	0	13
IoTSF 2.4.7.15	Where cryptographic suites are used such as TLS, all cipher suites shall be listed and validated against the current security recommendations such as NIST 800-131A [ref 2] or OWASP. Where insecure ciphers suites are identified they shall be removed from the product.	**2**	0	13
IoTSF 2.4.13.4	All the product related web servers' TLS certificate(s) are signed by trusted certificate authorities; are within their validity period; and processes are in place for their renewal.	**3**	0	12
IoTSF 2.4.13.6	The product related web servers support appropriately secure TLS/DTLS ciphers and disable/remove support for deprecated ciphers.	**2**	0	13
Qbit 4.7.5	**Vendors must be able to initiate firmware updates in IoT devices, either by automatic updates or by actively informing the user about availability of updates. The device must verify the authenticity and integrity of firmware updates before installing them.**	**0**	**0**	**15**
	Additionele vereisten uit IoTSF (niet gerelateerd aan Qbit-vereisten)	**10**	**1**	**183**
IoTSF 2.4.7.8	Where using initial pairing process, a Strong Authentication shall be used, requiring physical interaction with the device or possession of a shared secret.	0	1	14
IoTSF 2.4.7.19	Communications protocols should be latest versions with no publicly known vulnerabilities and/or appropriate for the product.	**2**	0	13
IoTSF 2.4.13.2	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.	**5**	0	10
IoTSF 2.4.13.17	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	**3**	0	12
Totaal		**22**	**1**	**676**

Op het gebied van wachtwoorden (Qbit-vereiste 1) stellen we vast dat alle behalve één product hier voldoen aan de eisen. Voor wat betreft authenticatie en blootstelling van poorten op het lokale netwerk (Qbit-vereiste 2 en 3) zien we zelfs alle apparaten voldoen. De versleuteling van netwerkverbindingen (Qbit-vereiste4) laat in sommige gevallen nog te wensen over. Als we hier naar de details kijken zien we dat met name het niet naleven van *best practices* op het gebied van met name TLS hiervoor de reden is.

Ten aanzien van het op afstand kunnen uitrollen van updates (Qbit-vereiste 5) hebben we geen afwijkingen geconstateerd. Hierbij merken we op dat het niet voor alle apparaten is vast komen te staan dat er een mogelijkheid *is* om deze op afstand bij te werken, omdat voor deze apparaten simpelweg geen updates beschikbaar zijn gekomen.

Tot slot zien we een aantal aandachtspunten bij de aanvullende (niet aan Qbit- relevante vereisten gerelateerde) aspecten, waarbij vooral op het aspect van het prijsgeven van versie-informatie een aantal apparaten niet voldoet aan de vereisten.

De ene babyfoon is de andere (niet)

Tijdens de test viel direct op dat de gebruikersapplicaties van de drie babyfoons in de steekproef sterk op elkaar leken. Ook voor wat betreft functionaliteit (denk bijvoorbeeld aan de wijze waarop de babyfoons gekoppeld dienden te worden aan de app) waren er grote gelijkenissen. We hebben het sterke vermoeden dat twee van de drie babyfoons (apparaat 4 en 6) zijn gebaseerd op een 'white label'-product van dezelfde leverancier. Ons vermoeden wordt gesterkt door het feit dat de versienummers van de apps voor deze apparaten vrijwel identiek waren (waarbij apparaat 4 consequent achterliep op apparaat 6 bij updates). De versienummers van de software op het apparaat daarentegen kenden een heel andere structuur.

We vermoeden dat de fabrikanten van apparaten 4 en 6 van de fabrikant van het white-labelproduct broncode krijgen, waarmee zij vervolgens zelf een update voor de software kunnen produceren en publiceren.

Hoewel ook apparaat 5 sterke gelijkenissen vertoonde met apparaten 4 en 6, lijkt het erop dat dit apparaat niet op dezelfde onderliggende (white label) software gebaseerd is (naar de hardware is in dit onderzoek niet gekeken, vanwege de keuze om de integriteit van de apparaten intact te laten).

De gelijkenissen tussen de apparaten maken het voor de consument lastig om te bepalen welk apparaat nu beter is in termen van (bijvoorbeeld) digitale veiligheid. Het is niet duidelijk of en hoe vaak de fabrikant updates zal uitbrengen en of deze dat sneller of minder snel zal doen dan de fabrikant van een ander, sterk vergelijkbaar apparaat.

4.5 Evaluatie van de methode

Na afloop van de gebruiksperiode is de testmethode door het onderzoeksteam geëvalueerd. Dit heeft geleid tot een aantal inzichten voor mogelijke verbetering ervan. Deze bevindingen kunnen relevant zijn voor herhaling van dit onderzoek in de toekomst.

4.5.1 Digitale veiligheid

Passendheid van het normenkader

De belangrijkste bevinding is dat het gebruikte controleraamwerk zich niet meer goed leent voor de (sterk op onlinediensten gebaseerde) architectuur die vandaag de dag door de meeste IoT-apparaten wordt gebruikt. Bijna alle apparaten worden geconfigureerd middels een mobiele app, communiceren via een versleutelde verbinding naar een eigen clouddienst en de gehele aansturing en informatieverwerking vindt plaats binnen de dienst

van de fabrikant. Lokale communicatie vindt nauwelijks meer plaats. We vermoeden daarnaast (dit is in het onderzoek nadrukkelijk niet gecontroleerd) dat steeds meer apparaten gebaseerd zijn op 'standaard' hardware/chipsets, met 'white label'-software(platforms), waarbij het onderscheidend vermogen zich bevindt in de clouddienst en niet-technische productkenmerken zoals de merknaam, de fysieke vorm en het uiterlijk van het apparaat.

Voor nieuwe onderzoeken zou ons inziens beter (met een iets lichtere testmethodiek) kunnen worden gekeken naar de "basis" beveiliging van de communicatie. De focus zou vervolgens moeten liggen op de clouddienst van de fabrikant. Deze kan uiteraard van buitenaf getest worden, maar er zou ook kunnen worden gewerkt met (bestaande) assurancerapportages.

Voor een volgend onderzoek adviseren wij concreet een *cloud assessment*-raamwerk (bijvoorbeeld CCM) op te nemen in de onderzoeksaanpak. Voor het testen van de SaaS-diensten van buitenaf is een vrijwaringverklaring nodig.

Technische opzet van de testomgeving

Ten aanzien van de technische opzet van de testomgeving komen we tot de volgende aanbevelingen:

- Het toepassen van TLS-interceptie leidt bij enkele apparaten tot problemen bij ingebruikname. Bij geen van de apparaten bleek het mogelijk om een eigen 'rootcertificaat' als vertrouwd in te voegen, waardoor apparaten weigerden de verbinding op te zetten. Hoewel het zinvol is om te controleren of apparaten dergelijke TLS-interceptie accepteren (en we verheugd zijn om te zien dat dit voor de apparaten in de steekproef niet mogelijk bleek!) is het voor toekomstige tests aan te bevelen dit pas ná ingebruikname en per apparaat te testen.

- Sommige apparaten verwachten dat het gebruikersapparaat met app zich op hetzelfde netwerk (Ethernetsegment) bevinden. Dit maakt het lastig(er) om het verkeer tussen applicatie en apparaat te analyseren op laag 3[93]. Het advies is hier om in toekomstige tests te overwegen monitoring op laag 2 te laten plaatsvinden (bijvoorbeeld middels een switch met *port mirroring*[94]).

- Niet alle apparaten (met name de wasmachines) houden de Wi-Fi-verbinding in stand wanneer zij in stand-bymodus staan. Dit maakt het lastig(er) om langer durende scans uit te voeren op deze apparaten. Bij sommige apparaten kon de "automatisch in stand-by"-functionaliteit worden uitgeschakeld. Voor een toekomstige test zou het zinvol kunnen zijn om (voor de andere apparaten) te werken met bijvoorbeeld tijdschakelaars, die ervoor zorgen dat apparaten op gezette tijden te maken krijgen met een stroomonderbreking.

---

[93] *Laag 3* verwijst naar de derde laag in het OSI-model (Open Systems Interconnection) van ISO. In dit model wordt netwerkverkeer logisch gescheiden in lagen, waarbij een hogere laag gebruik maakt van functionaliteit die door de laag eronder wordt geboden. De eerste laag is de fysieke laag (hieronder valt de elektrische signalering op bijvoorbeeld netwerkkabels). De tweede laag is de data-linklaag (hieronder valt bijvoorbeeld foutdetectie van uitgewisselde data). De derde laag is de netwerklaag. Op dit niveau vindt (bij IP) onder andere de routering van verkeer plaats (bijvoorbeeld de beslissing of een pakket binnen het lokale netwerk moet blijven of bestemd is voor een ander netwerk).

[94] Bij *port mirroring* kopieert de switch het verkeer dat via een specifieke set poorten wordt uitgewisseld naar een andere poort ter observatie.

Analyse van verzamelde gegevens

- Hoewel gedurende de testperiode alle netwerkverkeer is opgevangen (in zogenaamde PCAP-bestanden) bleek de verzamelde data minder waardevol dan vooraf gedacht. De meeste communicatie vindt versleuteld (met TLS) plaats. Het onderscheppen van het TLS-verkeer is nodig om dit te kunnen uitlezen (zie eerder).

- Het uitvoeren van Nessus-scans leidt tot veel verkeer dat eveneens wordt opgeslagen in de PCAP-bestanden. Dit maakt analyse daarvan lastiger. Een betere aanpak is wellicht om de Nessus-scans in een specifieke periode uit te voeren waarbinnen de logging van alle verkeer is uitgeschakeld.

Praktische overwegingen

Een aantal punten uit de evaluatie heeft te maken met de praktische uitvoerbaarheid van de voorgestelde testmethodiek:

- Een aantal apparaten vereist speciale hulpmiddelen bij installatie. Zo is voor de thermostaten over het algemeen nodig om zelf een netstroomkabel toe te voegen en elektrische verbindingen te maken (tussen thermostaat en bedieningskastje). Het bleek niet nodig om de thermostaten te verbinden aan een CV-ketel of (bij radiatorknoppen) een fysieke radiatorkraan. De wasmachines konden zonder water in gebruik worden genomen, maar omdat geen programma's konden worden gestart schakelden zij zich vaak binnen korte tijd weer in stand-bymodus.

- Door de grote verscheidenheid aan apparaten kostte ingebruikname, dagelijkse monitoring van de softwareversies en de analyse van de digitale veiligheid substantieel meer tijd dan initieel voorzien en begroot. Voor de initiële veiligheidstests waren 17 dagen begroot voor 15 apparaten (1 dag per apparaat plus rapportage en inrichting). Het advies is om dit ten minste te verdubbelen. Voor de overige analyses (compatibiliteit, functionaliteit, interoperabiliteit en het updatebeleid, in relatie tot informatieverstrekking) was voor de ingebruiknamefase 8 dagen begroot. We bevelen aan om hiervoor ten minste één dag per apparaat te reserveren.

5 Conclusie en aanbevelingen

In dit onderzoek staat centraal in welke mate domotica-apparaten die op de Nederlandse markt worden aangeboden voldoen aan wet- en regelgeving op het gebied van de compatibiliteit, functionaliteit, interoperabiliteit, het updatebeleid en de digitale veiligheid. In dit kader is een steekproef van 15 domotica-apparaten onderzocht. De steekproef bestond uit een zo gevarieerd mogelijke selectie van apparaten verdeeld over vijf productcategorieën. Hieronder beantwoorden we de onderzoeksvragen op basis van de steekproef. Vervolgens geven we aanbevelingen voor toekomstig onderzoek. De specifieke bevindingen per apparaat in de steekproef zijn te vinden in Bijlage 3.

5.1 Beantwoording onderzoeksvragen

5.1.1 Onderzoeksvraag 1. Hoe veilig is de software van domotica-apparaten op de Nederlandse markt?

Het basisniveau van digitale veiligheid van de software op de onderzochte domotica-apparaten is te typeren als voldoende, maar niet perfect:

- **Één domotica-apparaat in de steekproef bevatte een direct misbruikbare beveiligingszwakheid.** Bij de andere 14 domotica-apparaten zijn geen direct misbruikbare beveiligingszwakheden gevonden. In dit onderzoek is (op basis van het IoT Assurance Framework 3.0 [18] en de vereisten van Qbit [19]) primair gekeken naar beveiligingszwakheden die door een aanvaller met directe netwerktoegang tot het apparaat zouden zijn te misbruiken.

- **Voor acht apparaten in de steekproef stellen we vast dat niet wordt voldaan aan ten minste één vereiste uit de gehanteerde analyseraamwerken.** De gebreken betreffen het niet volgen van 'security best practices', waaronder met name de wijze van gebruik van TLS voor beveiliging van verbindingen en het prijsgeven van software- en versie-informatie. Dergelijke afwijkingen leiden niet direct tot een beveiligingsrisico, maar kunnen het aanvallers wel eenvoudiger maken er een te vinden. Mogelijk zegt het niet naleven van deze best practices iets over de wijze waarop de software wordt ontwikkeld: een assessment van de software door de fabrikant zou dergelijke 'best practices' mee moeten nemen, en in dat geval zouden we geen afwijkingen moeten vinden.

- **Domotica-apparaten maken in plaats van rechtstreekse communicatie over het lokale thuisnetwerk steeds vaker gebruik van een onlinedienst van de fabrikant. De digitale veiligheid is daardoor sterk(er) afhankelijk van deze onlinedienst.** Hoewel dit de veiligheid van de apparaten ten opzichte van een aanvaller met netwerktoegang tot het apparaat kan verhogen (vanwege het beperktere lokale aanvalsoppervlak), is de veiligheid wel sterk(er) afhankelijk van de veiligheid van de onlinedienst. De veiligheid van de onlinedienst is echter lastiger te controleren (en in dit onderzoek buiten scope gebleven).

- **Domotica-apparaten zijn voor ingebruikname vaak voorzien van relatief oude software. Niet alle[95] apparaten dwingen af dat de meest recente versie wordt geïnstalleerd bij ingebruikname.** Gebruikers kunnen daarom zonder het te weten gebruik maken van een verouderde, kwetsbare softwareversie.

- **Een aantal apparaten (specifiek de babyfoons in de steekproef) lijkt te zijn gebaseerd op 'white label' hard- en software. De merkleverancier past hierop niet alleen de eigen merknaam toe, maar maakt ook beslissingen die invloed hebben op de veiligheid**. Er zitten dan ook substantiële verschillen in updatebeleid en digitale veiligheid tussen apparaten die op het eerste gezicht technisch vrijwel identiek zijn.

Updates

- **In de steekproef ontvingen zeven van de 15 apparaten gedurende de gebruiksperiode geen enkele update (buiten een eventuele update direct na ingebruikname).** De bevindingen op het gebied van digitale veiligheid (zie hierboven) geven voor een aantal apparaten echter wel aanleiding tot het uitbrengen van een update.

- **Wanneer een apparaat wordt gebruikt in combinatie met een interoperabel apparaat van een andere fabrikant (zoals een domotica-basisstation) dan is niet gegarandeerd dat het apparaat (automatisch of handmatig) kan worden geüpdatet. Gebruikers kunnen daarom zonder het te weten gebruik maken van een verouderde, kwetsbare softwareversie.** In de steekproef bevond zich één dergelijke combinatie. In dit specifieke geval was ook het versienummer van de software op het apparaat niet zichtbaar. Deze beperking was in dit geval niet benoemd in de precontractueel beschikbare informatie.

5.1.2 Onderzoeksvraag 2. Welke informatie verstrekken de verkopers en de producenten van domotica-apparaten op de Nederlandse markt, en strookt dit met de daadwerkelijke kenmerken van het apparaat, en het daarna uitgevoerde updatebeleid?

Functionaliteit, compatibiliteit en interoperabiliteit

De door de verkopers en fabrikanten (precontractueel) verstrekte informatie over de functionaliteit, compatibiliteit en interoperabiliteit is summier:

- **Voor ieder online aangeschaft domotica-apparaat in de steekproef ontbrak ten minste één door ons onderzocht kenmerk ten aanzien van de functionaliteit, compatibiliteit en interoperabiliteit in de door de verkoper (precontractueel, tijdens ingebruikname en tijdens de gebruiksperiode) verstrekte informatie.** Dit geldt ook voor de informatie verstrekt door de fabrikant op moment van aankoop. In een klein aantal gevallen (van de gevallen waarin zowel verkoper als fabrikant informatie verstrekt over een kenmerk) *verschilt* de informatie die de verkoper verstrekt van de informatie van de fabrikant.

- **Bij aankopen in een fysieke winkel is de informatieverstrekking veel minder volledig, minder exact en gevarieerder dan bij online aankopen**, zelfs wanneer

[95] Een exact aantal is niet te geven omdat voor sommige apparaten in de steekproef geen update beschikbaar was op moment van ingebruikname. Op basis van dit onderzoek is niet te zeggen of deze apparaten het toepassen van een eventuele update bij ingebruikname zouden afdwingen als er wel een update beschikbaar zou zijn.

expliciet wordt gevraagd naar bijvoorbeeld de minimale updatetermijn. Voor de apparaten die zijn gekocht in een fysieke winkel was de verzamelde informatie niet geschikt voor verificatie, en geldt de bevinding hierboven in relatie tot de online verstrekte informatie (als ware het apparaat online gekocht).

- **De meeste domotica-apparaten in de steekproef zijn afhankelijk van een onlinedienst van de fabrikant voor het realiseren van slimme functionaliteit. Bij de meerderheid van de onderzochte apparaten is het voor de consument (precontractueel noch na ingebruikname) niet inzichtelijk tot wanneer de fabrikant deze dienst minimaal blijft aanbieden.** De mate waarin de apparaten afhankelijk zijn van de onlinedienst (welke functies niet beschikbaar zijn zonder onlinedienst) verschilt, waardoor er niet één aantal te geven is.

- **De online aangeschafte domotica-apparaten in de steekproef voldoen gedurende de onderzoeksperiode (op hoofdlijnen en voor zover wij konden beoordelen) wel aan wat in de verstrekte precontractuele informatie is beschreven over functionaliteit, compatibiliteit en interoperabiliteit.** We baseren dit op een controle van een vooraf gedefinieerde, niet-uitputtende set van zestien kenmerken. Noch direct na ingebruikname, noch na eventuele updates zijn door ons afwijkingen of wijzigingen geconstateerd voor deze eigenschappen.

Updatebeleid

De door de verkopers en fabrikanten (precontractueel) verstrekte informatie over het updatebeleid is summier:

- **Voor zes van de tien online aangeschafte apparaten is door de verkoper precontractueel geen informatie verstrekt over het updatebeleid. Bij vier online aankopen gaf de verkoper wel een termijn voor ondersteuning aan.** In het onderzoek is niet nagegaan of deze termijnen actueel en juist zijn. Aangezien de updates door de fabrikant worden ontwikkeld is de verkoper afhankelijk van informatieverstrekking hierover van de fabrikant.

- **Wanneer er (door de verkoper of de fabrikant) een minimumtermijn voor updates wordt verstrekt, is deze vaak relatief geformuleerd.** Duidelijker zou zijn om een concrete datum te noemen tot wanneer ondersteuning (minimaal) gegarandeerd wordt.

- **Voor slechts twee domotica-apparaten (van de acht online aangeschafte waarvoor dit van toepassing was) verstrekte de verkoper informatie over de specifieke (minimum)versienummers van besturingssystemen waarop de bijbehorende apps werken, terwijl deze ondersteuning gedurende de gebruikersperiode wel kan veranderen.** Voor acht domotica-apparaten (van de 12 die in combinatie met een app zijn onderzocht) is de minimumversie van het besturingssysteem voor de app verhoogd gedurende de meetperiode. Dit kan ertoe leiden dat oudere gebruikersapparaten niet meer kunnen worden gebruikt in combinatie met de meest recente versie van de app. In een klein aantal gevallen (van de gevallen waarin zowel verkoper als fabrikant de minimumversie verstrekken) verschilde het door de verkoper verstrekte minimumversienummer van dat van de fabrikant.

- **Een aantal apparaten kon pas worden bijgewerkt na acceptatie van voorwaarden.** Voor 11 van de 12 apparaten die met een app zijn getest, is het accepteren van gebruiksvoorwaarden in de app vereist voor ingebruikname. De updatefuncties zijn daarbij pas na het accepteren te benaderen in de app. De drie

televisies (die zonder app zijn getest) stellen de updatefunctie pas beschikbaar na het accepteren van voorwaarden op het televisiescherm. In het onderzoek is niet gecontroleerd of de apparaten zichzelf automatisch updaten zonder acceptatie van de voorwaarden. In de door verkoper en fabrikant verstrekte informatie is veelal niet duidelijk dat accepteren van de voorwaarden nodig is om de updatefunctie te kunnen benaderen. In sommige gevallen zijn de voorwaarden die worden weergegeven zelfs niet online vindbaar (zie Tabel 7). De voorwaarden zijn in dit onderzoek niet inhoudelijk gecontroleerd, omdat dit buiten de reikwijdte van het onderzoek valt.

5.2 Aanbevelingen ten aanzien van de werkwijze

- **Vanwege het doel en de wijze waarop de steekproef in dit onderzoek is samengesteld (met focus op onder andere variatie van technische eigenschappen) kan geen algemene uitspraak worden gedaan (in het bijzonder over afwezigheid van kwetsbaarheden) over domotica-apparaten op de Nederlandse markt.** Wanneer dit gewenst is adviseren we een onderzoeksopzet met een groter aantal vergelijkbare apparaten binnen een smallere categorie.

- **We adviseren om bij de beoordeling van de digitale veiligheid van domotica-apparaten gebruik te maken van een raamwerk dat past bij de (hedendaags dominante) architectuur waarin een clouddienst van de fabrikant centraal staat.** Er kan hierbij worden gewerkt met certificeringen. De dienst kan daarnaast van buitenaf getest worden (mits hiervoor vrijwaringsverklaringen zijn verkregen). Uiteraard blijft de veiligheid van het apparaat zélf daarbij van onverminderd groot belang. Daarnaast is relevant dat voor het updaten van de clouddienst soms ook een update van de software op het apparaat noodzakelijk zal zijn.

- **We adviseren om onderzoeken naar het updatebeleid van domotica-apparaten over een langere periode (bijvoorbeeld één of twee jaar) uit te voeren.** In dit onderzoek is het aantal updates gedurende de gebruiksperiode van drie maanden zeer beperkt. Met een meting over langere tijd kunnen met hogere zekerheid uitspraken worden gedaan over de consistentie van het updaten na het bekend worden van beveiligingszwakheden.

- **We adviseren nadere analyse van de voorwaarden die door gebruikers moeten worden geaccepteerd om slimme functies van het product te kunnen gebruiken.** Zonder het accepteren van de voorwaarden kan de updatefunctie en andere functies die afhankelijk zijn van de onlinedienst van de fabrikant veelal niet worden gebruikt. De voorwaarden zijn niet altijd vindbaar in de precontractuele fase.

Verwijzingen

[1] Europese Commissie (2022). *Gedelegeerde verordening (EU) 2022/30. Aanvulling van Richtlijn 2014/53/EU met betrekking tot de toepassing van de essentiële eisen* [eur-lex.europa.eu]

[2] Europese Commissie (2021). *Richtsnoeren met betrekking tot de uitlegging en toepassing van Richtlijn 2011/83/EG van het Europees Parlement en de Raad betreffende consumentenrechten*EU.

[3] Europese Commissie, DG Justitie (2014). *Leidraad betreffende Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten, tot wijziging van Richtlijn 93/13/EEG van de Raad en van Richtlijn 1999/44/EG van het Europees Parlement en de Raad en tot* [ec.europa.eu]

[4] Loos, M. (2018). *Algemene voorwaarden*Derde druk red., Den Haag: Boom juridische uitgevers.

[5] Strict (2019). *Report on IoT Device Security*Groningen: Agentschap Telecom.

[6] Kumar, S., Tiwari, P., en & Zymbler, M. (2019). *Internet of Things is a revolutionary approach for future technology enhancement: a review.* vol. 6, pp. 1-21.

[7] Multiscope (2021). *Helft huishoudens heeft smart home producten* [www.multiscope.nl]

[8] Multiscope (2021). *Categorieën* [www.multiscope.nl]

[9] IDC (2021). *IDC Forecasts Double-Digit Growth for Smart Home Devices as Consumers Embrace Home Automation and Ambient Computing* [www.idc.com]

[10] CBS (2021). *Bijna drie kwart van de Nederlanders maakt gebruik van slimme apparaten* [www.cbs.nl]

[11] van Trigt, M. (2016). *Dommer dan de diepvries* [www.vn.nl]

[12] GfK (2020). *GfK panelmarket Netherlands (periode januari 2020 t/m oktober 2020)*

[13] Su, B. (2008). *Characteristics of consumer search on-line: how much do we search?* vol. 13, pp. 109-129.

[14] Multiscope (2021). *Mannen het vaakst in bezit van smart home apparaten* [www.multiscope.nl]

[15] Dialogic, van der Vorst, T., Kats-Steur, J., Jelicic, N., en van Rees, J. (2019). *Mogelijkheden voor identificatie op internet op basis van IP-adres* [repository.wodc.nl] Den Haag: WODC.

[16] GfK (2020). *Smart Home in stroomversnelling door impact COVID-19 in Nederland* [www.gfk.com]

[17] Mavlanova, T., Benbunan-Fich, R., en & Koufaris, M. (2012). *Signaling theory and information asymmetry in online commerce* vol. 49, pp. 240-247.

[18]IoT Security Foundation (2021). *IoT Security Assurance Framework, Release 3.0, november 2021* [www.iotsecurityfoundation.org]

[19]Meulenhoff, P., Langkemper, S., en Westerhof, W. (2020). *Essential requirements for securing IoT consumer devices* [www.agentschaptelecom.nl]

[20]ETSI (2022). *Consumer IoT security* [www.etsi.org]

[21]ISO (2022). *ISO/IEC CD 27403.2. Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics* [www.iso.org]

[22]NIST (2022). *Official Common Platform Enumeration (CPE) Dictionary* [nvd.nist.gov]

[23]Spinner, Y. (2022). *Ubisoft haalt servers enkele oude games offline - update* [tweakers.net]

[24]Huijbregts, J. (2019). *Sony sluit servers voor PlayStation 4-game Driveclub eind maart 2020* [tweakers.net]

[25]Loos, M., en Pavillon, C. (2020). *Civielrechtelijke sancties op de schending van informatieplichten. Handvatten voor de ambtshalve toetsingspraktijk aan de Richtlijn consumentenrechten*p. 2128.

[26]Jongeneel, R. (2017). Zesde druk red., Deventer: Kluwer.

[27]Loos, M. (2019). *Consumentenkoop, Monografie BW B65b*Vierde druk red., Developer: Wolters Kluwer.

[28]Statcounter (2022). *Browser Market Share Netherlands* [gs.statcounter.com]

[29]Statista (2021). *Market share of web browsers in the Netherlands in 2021* [www.statista.com]

[30]Multiscope (2022). *Slimme huishoudelijke apparaten in opmars* [www.multiscope.nl]

[31]Google (2022). *How Chrome Incognito keeps your browsing private* [support.google.com]

Bijlage 1. Vragenlijst offline aankoop

1. Slimme verlichting

- Wat kan deze verlichting vergeleken met 'domme' verlichting?
- Kan ik de verlichting op afstand besturen? En met welk apparaat?
    - Telefoon? Stem?
- Hoe zit het met updates?
    - Hoe lang? Belangrijk?
- Hoe zit het met veiligheid?

2. Slimme babyfoon

- Wat kan deze babyfoon vergeleken met een 'domme' babyfoon?
- Kan ik de babyfoon op afstand besturen? En met welk apparaat?
- Kan ik op afstand het beeld van de camera zien?
- Hoe zit het met updates?
    - Hoe lang? Belangrijk?
- Hoe zit het met veiligheid?

3. Smart tv

- Op welk besturingssysteem draait de tv? Kan het bepaalde dingen wel of niet?
- Kan ik de tv met elke smartphone bedienen?
- Verbinden met (elke) smart home?
- Hoe zit het met updates?
    - Hoe lang? Belangrijk?
- Hoe zit het met veiligheid?

4. Slimme thermostaat

- Wat kan deze thermostaat vergeleken met een 'domme' thermostaat?
- Kan ik de thermostaat op afstand besturen? En met welk apparaat?
    - Telefoon? Stem?
- Kan ik de temperatuur per kamer regelen?
- Hoe zit het met updates?
    - Hoe lang? Belangrijk?
- Hoe zit het met veiligheid?

5. Slimme wasmachine

- Wat kan deze wasmachine vergeleken met een 'domme' wasmachine?
- Kan ik de wasmachine op afstand besturen? En met welk apparaat?
- Kan hij verbinden met Alexa of Google home?
- Hoe zit het met updates?
    - Hoe lang? Belangrijk?
- Hoe zit het met veiligheid?

Bijlage 2. Uitwerking raamwerk analyse digitale veiligheid

In de onderstaande tabel is het normenkader voor de security-analyse in dit onderzoek opgenomen. Het normenkader is gebaseerd op het "IoT Assurance Framework 3.0" d.d. november 2021 [18] en de "essential requirements" van Qbit. [19] De normen die passen binnen de scope (zie paragraaf 3.7.1) en kunnen worden getoetst binnen dit onderzoek met deze apparaatselectie zijn opgenomen in het normenkader. Daarbij is ook het moment van testen gespecifieerd. De IoTSF-vereisten zijn gegroepeerd naar Qbit-vereiste. De Qbit-vereisten worden ook zelfstandig getest.

Control	Beschrijving	Moment van testen	Testactiviteit
Qbit 4.7.1	**All passwords must conform to the industry standard NIST SP800-63b Digital Identity Guidelines.**	**Initiële en periodieke scan**	**Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.**
IoTSF 2.4.6.3	All unnecessary accounts or logins have been disabled or eliminated from the software at the end of the software development process, e.g. development or debug accounts and tools.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.8.3	Where a user interface password is used for login authentication, the factory issued or reset password is randomly unique for every device in the product family. If a passwordless authentication is used the same principles of uniqueness apply.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.8.4	The product does not accept the use of null or blank passwords	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.8.6	Password entry follows industry standard practice on password length, characters from the groupings and special characters.	Initiële scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.8.7	The product has defence against brute force repeated login attempts, such as exponentially increasing retry attempt delays.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.8.11	The product only allows controlled user account access; access using anonymous or guest user accounts is not supported without justification	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.

Control	Beschrijving	Moment van testen	Testactiviteit
IoTSF 2.4.8.12	The product allows the factory issued or OEM login accounts to be disabled or erased or renamed when installed or commissioned.	Initiële scan	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.8.13	The product supports having any or all of the factory default user login passwords altered when installed or commissioned.	Additionele security-analyse (penetratietest).	Analyse van het apparaat
IoTSF 2.4.13.11	All the related servers and network elements prevent the use of null or blank passwords.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.14	All the related servers and network elements enforce passwords that follows industry good practice.	Additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.15	Brute force attacks are impeded by introducing escalating delays following failed user account login attempts, and/or a maximum permissible number of consecutive failed attempts.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
Qbit 4.7.2	**Access to device functionality via a network interface in the initialised state must only be possible after authentication on that interface.**	**Initiële en periodieke scan**	**Poortscan en netwerkanalyse**
IoTSF 2.4.5.5	If the product has any virtual port(s) that are not required for normal operation, they are only allowed to communicate with authorised and authenticated entities or are securely disabled when shipped. When a port is initialised or used for field diagnostics, the port input commands are deactivated and the output provides no information which could compromise the device, such as credentials, memory address or function names.	Initiële en periodieke scan	Poortscan en penetratietest
IoTSF 2.4.5.21	Where the device software communicates with a product related webserver or application over TCP/IP or UDP/IP, the device software uses certificate pinning or public/private key equivalent, where appropriate.	Additionele security-analyse (penetratietest).	Geautomatiseerde security scan en manuele penetratietest.
IoTSF 2.4.7.7	If a connection requires a password or passcode or passkey for connection authentication, the factory issued or reset password is unique to each device.	Additionele security-analyse (penetratietest).	Manuele penetratietest.
IoTSF 2.4.10.2	Where the product or service provides a web browser-based interface, access to any restricted/administrator area or functionality shall require authentication.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.10.13	Administration Interfaces are accessible only by authorized operators. Mutual Authentication is used over administration	Additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.

Control	Beschrijving	Moment van testen	Testactiviteit
	interfaces, for example, by using certificates.		
IoTSF 2.4.11.12	Access to device functionality via a network/web browser interface in the initialized state should only be permitted after successful Authentication using current best practice secure cryptographic modules.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
Qbit 4.7.3	**All exposed ports and interfaces must be necessary for the normal and intended use of the device.**	**Initiële en periodieke scan**	**Poortscan en netwerkanalyse**
IoTSF 2.4.4.5	Any debug interface only communicates with authorised and authenticated entities on the production devices. The functionality of any interface should be minimised to its essential task(s).	Initiële en periodieke scan	Poortscan en netwerkanalyse
IoTSF 2.4.4.9	All communications port(s) which are not used as part of the product's normal operation are not physically accessible or only communicate with authorised and authenticated entities.	Initiële en periodieke scan	Poortscan en netwerkanalyse
IoTSF 2.4.4.10	All the product's development test points are securely disabled or removed wherever possible in production devices.	Initiële en periodieke scan	Poortscan en netwerkanalyse
IoTSF 2.4.7.6	All the product's unused ports (or interfaces) are closed and only the necessary ones are active.	Initiële en periodieke scan	Poortscan en penetratietest
IoTSF 2.4.7.18	The product only initialises and enables the communications interfaces, network protocols, application protocols and network services necessary for the product's operation.	Periodieke analyse van netwerkverkeer	Analyse van netwerkverkeer
Qbit 4.7.4	**All network traffic must be encrypted and authenticated using best practice encryption protocols, such as TLS.**	**Periodieke scan, periodieke analyse netwerkverkeer en additionele security-analyse (penetratietest).**	**Analyse van netwerkverkeer**
IoTSF 2.4.7.4	Devices support only the versions of application layer protocols that have been reviewed and evaluated against publicly known vulnerabilities.	Periodieke analyse van netwerkverkeer	Analyse van netwerkverkeer
IoTSF 2.4.7.13	Where a TCP protocol, such as MQTT, is used, it is protected by a TLS connection with no known vulnerabilities.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.7.14	Where a UDP protocol is used, such as CoAP, it is protected by a DTLS connection with no known vulnerabilities.	Periodieke analyse van netwerkverkeer	Analyse van netwerkverkeer
IoTSF 2.4.7.15	Where cryptographic suites are used such as TLS, all cipher suites shall be listed and validated against the current security recommendations such as NIST 800-131A	Periodieke scan, periodieke analyse netwerkverkeer en additionele security-	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.

Control	Beschrijving	Moment van testen	Testactiviteit
	[ref 2] or OWASP. Where insecure ciphers suites are identified they shall be removed from the product.	analyse (penetratietest).	
IoTSF 2.4.7.16	All use of cryptography by the product, such as TLS cipher suites, shall be listed and validated against the import/export requirements for the territories where the product is to be sold and/or shipped.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.7.20	Post product launch, communications protocols should be reviewed throughout the product life cycle against publicly known vulnerabilities and changed to the most secure versions available if appropriate.	Periodieke analyse van netwerkverkeer	Analyse van netwerkverkeer
IoTSF 2.4.10.1	Where the product or service provides a webbased user interface, Authentication is secured using current best practice cryptography.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.10.3	Where the product or service provides a webbased management interface, Authentication is secured using current best practice cryptography.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.10.19	Any personal data communicated between the web interface and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	Periodieke scan en additionele security-analyse (penetratietest).	Poortscan en penetratietest
IoTSF 2.4.11.4	Where the application communicates with a product related remote server(s), or device, it does so over a secure connection.	Periodieke analyse van netwerkverkeer	Analyse van netwerkverkeer
IoTSF 2.4.11.13	Any personal data communicated between the mobile app and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	Periodieke analyse van netwerkverkeer	Analyse van netwerkverkeer
IoTSF 2.4.13.4	All the product related web servers' TLS certificate(s) are signed by trusted certificate authorities; are within their validity period; and processes are in place for their renewal.	Initiële scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.6	The product related web servers support appropriately secure TLS/DTLS ciphers and disable/remove support for deprecated ciphers.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.7	The product related web servers have repeated renegotiation of TLS connections disabled.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.10	Where a product related to a webserver encrypts communications using TLS, certificate pinning is implemented.	Initiële scan en additionele security-analyse (penetratietest).	Analyse van netwerkverkeer

Control	Beschrijving	Moment van testen	Testactiviteit
IoTSF 2.4.13.23	If run as a cloud service, the cloud service TCP based communications (such as MQTT connections) are encrypted and authenticated using the latest TLS standard.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.24	If run as a cloud service, UDP-based communications are encrypted using the latest Datagram Transport Layer Security (DTLS)	Periodieke analyse van netwerkverkeer	Analyse van netwerkverkeer
Qbit 4.7.5	**Vendors must be able to initiate firmware updates in IoT devices, either by automatic updates or by actively informing the user about availability of updates.** **The device must verify the authenticity and integrity of firmware updates before installing them.**	**Periodieke analyse van netwerkverkeer en het update-bestand**	**Analyse van netwerkverkeer en manuele penetratietest**
IoTSF 2.4.5.2	Where remote software updates can be supported by the device, the software images must be digitally signed by an appropriate signing authority - e.g. manufacturer/supplier or public. The Signing Authority should be clearly identified.	Periodieke analyse van netwerkverkeer en het update-bestand	Analyse van netwerkverkeer en manuele penetratietest
IoTSF 2.4.5.3	Where updates are supported, the software update package has its digital signature, signing certificate and signing certificate chain verified by the device before the update process begins.	Periodieke analyse van netwerkverkeer en het update-bestand	Analyse van netwerkverkeer en manuele penetratietest
IoTSF 2.4.5.4	If remote software upgrade is supported by a device, software images shall be encrypted or transferred over an encrypted channel.	Periodieke analyse van netwerkverkeer	Analyse van netwerkverkeer
Additionele vereisten uit IoTSF (niet gerelateerd aan Qbit-vereisten)			
IoTSF 2.4.7.8	Where using initial pairing process, a Strong Authentication shall be used, requiring physical interaction with the device or possession of a shared secret.	Additionele security-analyse (penetratietest).	Analyse van het apparaat
IoTSF 2.4.7.9	Where a wireless interface has an initial pairing process, the passkeys are changed from the factory issued, or reset password prior to providing normal service.	Additionele security-analyse (penetratietest).	Analyse van het apparaat
IoTSF 2.4.7.19	Communications protocols should be latest versions with no publicly known vulnerabilities and/or appropriate for the product.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.8.14	If the product has a password recovery or reset mechanism, an assessment has been made to confirm that this mechanism	Additionele security-analyse (penetratietest).	Analyse van het apparaat

Control	Beschrijving	Moment van testen	Testactiviteit
	cannot readily be abused by an unauthorised party.		
IoTSF 2.4.8.16	The product allows an authorised and complete factory reset of all of the device's authorisation information.	Additionele security-analyse (penetratietest).	Analyse van het apparaat
IoTSF 2.4.10.4	Where a web user interface password is used for login authentication, the initial password or factory reset password is unique for every device in the product family.	Additionele security-analyse (penetratietest).	Analyse van het apparaat
IoTSF 2.4.10.5	The web user interface is protected by an automatic session idle logout timeout function.	Additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.10.11	Sanitize input in Web applications by using URL encoding or HTML encoding to wrap data and treat it as literal text rather than executable script	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.10.12	All inputs and outputs are validated using for example an allow list (formerly 'whitelist') containing authorised origins of data and valid attributes of such data.	Additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.10.14	Reduce the lifetime of sessions to mitigate the risk of session hijacking and replay attacks. (For example, to reduce the time an attacker has to capture a session cookie and use it to access an application).	Additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.10.15	All inputs and outputs are checked for validity. Tests to include both expected (valid) and unexpected (invalid) input stimuli.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.2	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.3	All product related web servers have their webserver HTTP trace and trace methods disabled	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.17	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	Additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.
IoTSF 2.4.13.18	All the related servers and network elements prevent anonymous/guest access except for read only access to public information.	Periodieke scan en additionele security-analyse (penetratietest).	Geautomatiseerde security scan, manuele penetratietest en vulnerability scanning.

Bijlage 3. Bevindingen per apparaat

In deze bijlage geven we per apparaat de belangrijkste bevindingen.

Bij de in dit hoofdstuk gepresenteerde resultaten dienen de volgende belangrijke kanttekeningen te worden geplaatst:

- De meting betreft een momentopname die onder zeer specifieke omstandigheden is uitgevoerd.
- Voor veel van de hier onderzochte zaken geldt dat het (theoretisch en praktisch gezien) niet mogelijk is om 100% uitsluitsel te geven. Een positieve score op het aspect digitale veiligheid betekent niet per definitie dat het apparaat 100% veilig is.

Apparaat 1. [redacted] lamp

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 3 criteria werd niet voldaan. Aan 21 criteria werd voldaan. 23 criteria zijn niet van toepassing. Niet-conform criteria: IoTSF 2.4.13.4, IoTSF 2.4.13.2, IoTSF 2.4.13.17
Compatibiliteit	De minimumversie van Android/iOS voor de bijbehorende app is niet gewijzigd gedurende de test (geen updates app).
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	Clouddienst lijkt nodig om apparaat te kunnen gebruiken (geen modus die alleen lokaal werkt)
Updatebeleid	Direct na ingebruikname was een update beschikbaar, die de gebruiker weliswaar handmatig dient te installeren.

Apparaat 2. [redacted] lamp

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 5 criteria werd niet voldaan. Aan 20 criteria werd voldaan. 21 criteria zijn niet van toepassing. Niet-conform criteria: IoTSF 2.4.7.13, IoTSF 2.4.7.15, IoTSF 2.4.13.4, IoTSF 2.4.13.6, IoTSF 2.4.7.19
Compatibiliteit	De minimumversie van Android/iOS voor de bijbehorende app is niet gewijzigd gedurende de test.
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.

Aspect	Belangrijkste bevindingen - na ingebruikname
Functionaliteit	Clouddienst lijkt niet nodig om apparaat te kunnen gebruiken.
Updatebeleid	Tijdens ingebruikname vereiste de applicatie dat een update werd geïnstalleerd voordat het apparaat verder in gebruik kon worden genomen.

Apparaat 3. [redacted] lamp

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan geen enkel criterium werd niet voldaan. Aan 22 criteria werd voldaan. 23 criteria zijn niet van toepassing. Aan 1 criterium werd voldaan met een waarschuwing.
Compatibiliteit	De minimumversie voor de Android-app is gedurende de testperiode gewijzigd van 6.0 naar 8.0.
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	Clouddienst lijkt nodig om het apparaat te kunnen gebruiken (geen modus die alleen lokaal werkt)
Updatebeleid	De [redacted]-applicatie toont niet het versienummer van de gekoppelde Hue-lamp. De [redacted] lijkt niet te beschikken over de mogelijkheid om de [redacted] te updaten. Het is technisch gezien mogelijk om deze updates uit te voeren (hiervoor zou waarschijnlijk eerst een update van de software op de [redacted] en de app nodig zijn).

Apparaat 4. [redacted] Babyfoon

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 2 criteria werd niet voldaan. Aan 22 criteria werd voldaan. 23 criteria zijn niet van toepassing. Niet-conform criteria: IoTSF 2.4.13.2, IoTSF 2.4.13.17
Compatibiliteit	De minimumversie van iOS voor de bijbehorende app is niet gewijzigd gedurende de test. De minimumversie voor Android is gewijzigd van 4.4 naar 5.0.
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	Clouddienst lijkt nodig om het apparaat in gebruik te nemen, maar het apparaat werkt waarschijnlijk ook binnen het lokale netwerk zonder deze dienst.
Updatebeleid	• Geen updates beschikbaar van de 'firmware' direct na ingebruikname. Dit is opvallend, gegeven het feit dat het apparaat in januari 2021 is uitgebracht en dus al een

Aspect	Belangrijkste bevindingen - na ingebruikname
	tijdje 'in de schappen' zou hebben kunnen liggen. De app is in de eerste twee weken na ingebruikname wel enige malen bijgewerkt. • De babyfoon lijkt gebaseerd te zijn op exact hetzelfde [redacted]-platform als de [redacted] (apparaat 6). De versienummers van de apps lijken op elkaar, maar zijn niet altijd gelijk. In de eerste twee weken is de [redacted]-app bijgewerkt naar versie 3.38.0 terwijl de [redacted]-applicatie tot twee dagen na dat moment nog 3.37.2 was. Ook eerder zien we dat de updatefrequentie verschilt. De versienummers van de 'firmware' verschillen, en er zijn nog geen updates beschikbaar komen; het is daarom lastig vast te stellen in hoeverre deze met elkaar 'in de pas' lopen.
Overig	De fabrikant [redacted] heeft geen eigen website. Het lijkt een 'white label'-merk op een apparaat dat in de basis werkt op basis van het [redacted]-platform.

Apparaat 5. [redacted] babyfoon

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 5 criteria werd niet voldaan. Aan 28 criteria werd voldaan. 13 criteria zijn niet van toepassing. Niet-conform criteria: IoTSF 2.4.8.5, IoTSF 2.4.8.6, IoTSF 2.4.8.7, IoTSF 2.4.13.2, IoTSF 2.4.13.17. Dit apparaat bevatte een concrete serieuze beveiligingszwakheid: het apparaat verstuurde onversleutelde camera-afbeeldingen naar een server op internet. Dit is gemeld bij de fabrikant.
Compatibiliteit	De minimumversie van de iOS-app is gedurende de testperiode gewijzigd van iOS 9.0 naar iOS 10.0.
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	Clouddienst lijkt nodig om apparaat in gebruik te nemen, maar het apparaat werkt waarschijnlijk ook binnen het lokale netwerk zonder deze dienst.
Updatebeleid	• Geen updates van de 'firmware' beschikbaar direct na ingebruikname. Dit is opvallend, gegeven het feit dat het apparaat in januari 2021 is uitgebracht en dus al een tijdje 'in de schappen' zou hebben kunnen gelegen. De app is in de eerste twee weken na ingebruikname wel enige malen bijgewerkt. • Hoewel de app sterk lijkt op die van de andere geteste babyfoons ontbreekt in deze app vreemd genoeg de optie om automatische updates in te schakelen of een handmatige controle up updates te starten. De [redacted]

Aspect	Belangrijkste bevindingen - na ingebruikname
	versienummers zijn in hetzelfde scherm echter wel zichtbaar en de indruk wordt gewekt dat deze versies 'up-to-date' zijn.
Overig	Het is niet duidelijk wie de fabrikant van dit apparaat is. Het apparaat werkt op basis van het '[redacted]'-platform. Het ogenschijnlijk zelfde apparaat wordt onder meerdere namen (o.a. '[redacted]') verkocht. De [redacted]-app wordt in de Apple App Store aangeboden op naam van een persoon, en er lijkt een connectie te zijn met het bedrijf [redacted].

Apparaat 6. [redacted] babyfoon

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 23 criteria werd voldaan. 23 criteria zijn niet van toepassing.
Compatibiliteit	De minimumversie voor de Android-app is gedurende de testperiode gewijzigd van 4.4 naar 5.0.
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	Clouddienst lijkt nodig om apparaat in gebruik te nemen, maar het apparaat werkt waarschijnlijk ook binnen het lokale netwerk zonder deze dienst.
Updatebeleid	• Geen updates van de 'firmware' beschikbaar direct na ingebruikname. Dit is opvallend, gegeven het feit dat het apparaat in januari 2021 is uitgebracht en dus al een tijdje 'in de schappen' zou hebben kunnen gelegen. De app is in de eerste twee weken na ingebruikname wel enige malen bijgewerkt. • De babyfoon lijkt gebaseerd te zijn op exact hetzelfde [redacted]-platform als de [redacted]-babyfoon (apparaat 4). De versienummers van de apps lijken op elkaar, maar zijn niet altijd gelijk. In de eerste twee weken is de [redacted]-app bijgewerkt naar versie 3.38.0 terwijl de [redacted]-applicatie tot twee dagen na dat moment nog 3.37.2 was. Ook eerder zien we dat de updatefrequentie verschilt. De versienummers van de 'firmware' verschillen, en er zijn nog geen updates beschikbaar komen; het is daarom lastig vast te stellen in hoeverre deze met elkaar 'in de pas' lopen.

Apparaat 7. [redacted] TV

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 23 criteria werd voldaan. 24 criteria zijn niet van toepassing.
Compatibiliteit	(Apparaat functioneert zelfstandig)

Aspect	Belangrijkste bevindingen - na ingebruikname
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	Kernfuncties zijn te gebruiken zonder gebruik te maken van clouddiensten van de fabrikant.
Updatebeleid	• Het apparaat kan pas worden bijgewerkt nadat algemene voorwaarden en een privacyovereenkomst (op het apparaat zelf) zijn geaccepteerd. Het lezen van deze (lange) overeenkomsten is alleen mogelijk op het scherm en voor een consument niet erg prettig. • Kort na ingebruikname is een update beschikbaar gekomen. • Hoewel de televisie 'automatisch bijwerken' ondersteunt, is niet duidelijk of de televisie controleert op updates wanneer deze in stand-by staat.

Apparaat 8. [redacted] TV

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 6 criteria werd niet voldaan. Aan 16 criteria werd voldaan. 25 criteria zijn niet van toepassing. Niet-conform criteria: IoTSF 2.4.7.13, IoTSF 2.4.7.15, IoTSF 2.4.13.4, IoTSF 2.4.13.6, IoTSF 2.4.7.19, IoTSF 2.4.13.2
Compatibiliteit	(Apparaat functioneert zelfstandig)
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	• Kernfuncties te gebruiken zonder gebruik te maken van clouddiensten van de fabrikant. • Verkoper geeft aan niet te kunnen garanderen dat apps die op de afbeelding van het apparaat worden getoond blijven werken; dit ligt bij de fabrikant.
Updatebeleid	• Het apparaat kan pas worden bijgewerkt nadat algemene voorwaarden en een privacyovereenkomst (op het apparaat zelf) zijn geaccepteerd. Het lezen van deze (lange) overeenkomsten is alleen mogelijk op het scherm en voor een consument niet erg prettig. • Kort na ingebruikname is een update beschikbaar gekomen. • Hoewel de televisie 'automatisch bijwerken' ondersteunt, is niet duidelijk of de televisie controleert op updates wanneer deze in stand-by staat.

Apparaat 9. [redacted] TV

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 22 criteria werd voldaan. 25 criteria zijn niet van toepassing.
Compatibiliteit	(Apparaat functioneert zelfstandig)
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	Kernfuncties te gebruiken zonder gebruik te maken van clouddiensten van de fabrikant.
Updatebeleid	• Kort na ingebruikname is een update beschikbaar gekomen. • Hoewel de televisie 'automatisch bijwerken' ondersteunt, is niet duidelijk of de televisie controleert op updates wanneer deze in stand-by staat.
Overig	• Voor dit specifieke apparaat was geen fabrikantpagina vindbaar (volgens de beschreven testmethode).

Apparaat 10. [redacted] thermostaat

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 23 criteria werd voldaan. 23 criteria zijn niet van toepassing.
Compatibiliteit	De minimumversie van Android/iOS voor de bijbehorende app is niet gewijzigd gedurende de test.
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	De clouddienst van [redacted] is nodig om het apparaat in gebruik te kunnen nemen.
Updatebeleid	• Kort na ingebruikname is een update beschikbaar gekomen voor de via ZigBee verbonden onderdelen (thermostaat en radiatorknoppen). Voor zover bekend is de firmware op de 'internet bridge' niet bijgewerkt na ingebruikname. • Het is niet duidelijk in hoeverre het apparaat (specifiek de 'internet bridge') in staat is om automatisch en zonder tussenkomst van de app updates binnen te halen en te installeren.

Apparaat 11. [redacted] thermostaat

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 24 criteria werd voldaan. 23 criteria zijn niet van toepassing.
Compatibiliteit	De minimumversie van iOS die nodig is om de bijbehorende app te kunnen gebruiken is verhoogd van iOS 12 naar 13.
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	Kernfuncties zijn te gebruiken zonder gebruik te maken van clouddiensten van de fabrikant.
Updatebeleid	• De firmware van de thermostaat is na ingebruikname niet bijgewerkt, en er is geen nieuwere versie beschikbaar. Dit is opvallend, aangezien dit apparaat al langere tijd op de markt is, en het goed mogelijk is dat het geteste exemplaar al enige tijd 'in de schappen' ligt. • De thermostaat lijkt zelf niet in staat om automatisch updates binnen te halen en te installeren. De applicatie biedt geen optie tot automatisch updaten noch tot handmatig initiëren van een updatecontrole.

Apparaat 12. [redacted] thermostaat

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 23 criteria werd voldaan. 24 criteria zijn niet van toepassing.
Compatibiliteit	Apparaat is zelfstandig te gebruiken. De minimumversie van Android voor de bijbehorende app is gedurende de testperiode gewijzigd van 6.0 naar 8.0.
Interoperabiliteit	Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen.
Functionaliteit	Kernfuncties te gebruiken zonder gebruik te maken van clouddiensten van de fabrikant.
Updatebeleid	De thermostaat kan zelfstandig (zonder tussenkomst van een app) automatisch updates downloaden en installeren. • Kort na ingebruikname is een update beschikbaar gekomen voor de thermostaat. • Via het menu van de thermostaat kan worden gecontroleerd wanneer een update is geïnstalleerd.

Apparaat 13. [redacted] wasmachine

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 25 criteria werd voldaan. 21 criteria zijn niet van toepassing.
Compatibiliteit	De minimumversie van iOS die nodig is om de bijbehorende app te kunnen gebruiken is verhoogd van iOS 11 naar 12.
Interoperabiliteit	• Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen. • Het koppelen met Wi-Fi-netwerken blijkt bij de wasmachines in het algemeen (o.a. vanwege de beperkte interface op het apparaat en de koppelmethode) vaker te mislukken om onduidelijke redenen.
Functionaliteit	Kernfuncties te gebruiken zonder gebruik te maken van clouddiensten van de fabrikant.
Updatebeleid	• Kort na ingebruikname is een update beschikbaar gekomen en geïnstalleerd. • De wasmachine lijkt niet in staat om zelfstandig (zonder tussenkomst van de app) een update te downloaden en te installeren. Een euvel dat alle wasmachines treft is dat zij niet altijd verbonden lijken te zijn met het Wi-Fi-netwerk.

Apparaat 14. [redacted] wasmachine

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 26 criteria werd voldaan. 21 criteria zijn niet van toepassing.
Compatibiliteit	De minimumversie van Android/iOS voor de bijbehorende app is niet gewijzigd gedurende de test (geen updates app).
Interoperabiliteit	• Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen. • Het koppelen met Wi-Fi-netwerken blijkt bij de wasmachines in het algemeen (o.a. vanwege de beperkte interface op het apparaat en de koppelmethode) vaker te mislukken om onduidelijke redenen. • Deze wasmachine lijkt regelmatig verbinding te verliezen met het Wi-Fi-netwerk (ondanks dat het display aangeeft dat er nog wel verbinding is), waarna de applicatie de wasmachine niet meer kan vinden.
Functionaliteit	• Kernfuncties te gebruiken zonder gebruik te maken van clouddiensten van de fabrikant.

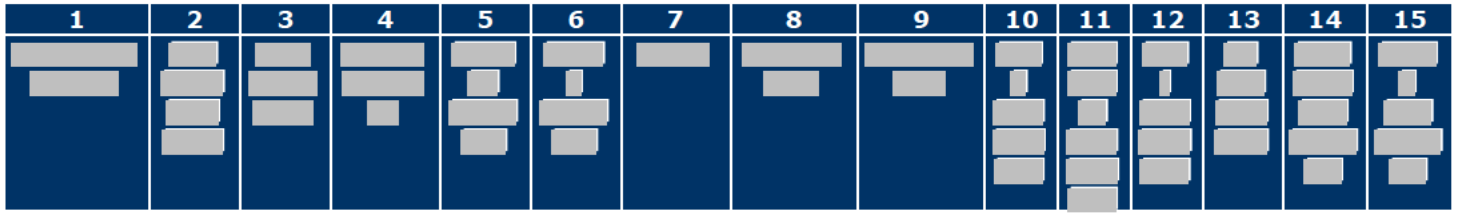
Aspect	Belangrijkste bevindingen - na ingebruikname
Updatebeleid	• De wasmachine lijkt niet in staat om zelfstandig (zonder tussenkomst van de app) een update te downloaden en te installeren. Een euvel dat alle wasmachines treft is dat zij niet altijd verbonden lijken te zijn met het Wi-Fi-netwerk. • Hoewel de bijbehorende '[redacted]'-app niet is geupdate, werden onderdelen van deze app gedurende de test ogenschijnlijk wel geüpdatet ("nieuwe controller beschikbaar").

Apparaat 15. [redacted] wasmachine

Aspect	Belangrijkste bevindingen - na ingebruikname
Digitale veiligheid	Aan 1 criterium werd niet voldaan. Aan 24 criteria werd voldaan. 22 criteria zijn niet van toepassing. Niet-conform criteria: IoTSF 2.4.13.2
Compatibiliteit	De minimumversie van iOS die nodig is om de bijbehorende app te kunnen gebruiken is verhoogd van iOS 13 naar 14.
Interoperabiliteit	• Het apparaat interopereert naar behoren in de testomgeving. Hoewel interoperabiliteit niet volledig testbaar is, zijn er uit de test geen redenen om aan te nemen dat de interoperabiliteit afwijkt van hetgeen door de verkoper precontractueel is aangegeven naar voren gekomen. • Het koppelen met Wi-Fi-netwerken blijkt bij de wasmachines in het algemeen (o.a. vanwege de beperkte interface op het apparaat en de koppelmethode) vaker te mislukken om onduidelijke redenen.
Functionaliteit	Kernfuncties zijn te gebruiken zonder gebruik te maken van clouddiensten van de fabrikant.
Updatebeleid	• De wasmachine lijkt niet in staat om zelfstandig (zonder tussenkomst van de app) een update te downloaden en te installeren. Een euvel dat alle wasmachines treft is dat zij niet altijd verbonden lijken te zijn met het Wi-Fi-netwerk.

Overzichten resultaten individuele apparaten

Tabel 11 Overzicht resultaten onderzoek rondom updatebeleid per apparaat

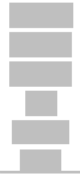


	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Feitelijke eigenschappen apparaat met betrekking tot het updatebeleid															
Firmware (software op het apparaat)															
Mogelijkheid tot handmatig updaten (evt. via app)	Ja	Ja	Nee	Ja	Nee	Ja	Ja	Ja	Ja	Ja	Nee	Ja	Nee	Nee	Nee
Mogelijkheid om automatisch updaten in te schakelen (evt. via app)	Nee	Ja	Nee	Ja	Nee	Ja	Ja	Ja	Ja	Nee	Nee	Ja	Nee	Nee	Nee
Update mogelijk zonder gebruik app	Nee	Ja	Nee	Nee	Onbekend	Nee	Ja	Ja	Ja	Nee	Nee	Ja	Onbekend	Onbekend	Onbekend
Forceert eerste update bij ingebruikname	Nee	Ja	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee
Automatisch updaten standaard ingeschakeld	Nee	Ja[96]	Nee	Nee	Onbekend	Nee	Nee	Nee	Nee[97]	Nee	Nee	Ja	Onbekend	Onbekend	Onbekend
Kan gekoppelde apparaten (ZigBee e.a.) bijwerken	Ja[98]	Ja	Nee	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	Ja	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.

[96] Voorstel tijdens installatie dat kan worden geweigerd door de gebruiker.

[97] De functie om een melding te tonen bij beschikbaarheid van een update is wel standaard ingeschakeld.

[98] De applicatie wekt deze indruk, maar we hebben gedurende de gebruiksperiode geen dergelijke update waargenomen.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
															
Bijzonderheden							*99	*100	*101						
Datum volledige ingebruikname	30-3-2022	30-3-2022	25-3-2022	25-3-2022	25-3-2022	25-3-2022	25-3-2022	25-3-2022	25-3-2022	30-3-2022	22-3-2022	22-3-2022	25-3-2022	30-3-2022	28-3-2022
Versie firmware bij ingebruikname															
App															
Aantal updates app van 01-04-22 t/m 30-06-22	0	7[102]	n.b.[103]	7	2	7	n.v.t.	n.v.t.	n.v.t.	16	3	n.v.t.	4[104]	3[105]	0[106]

[99] Vereist lezen en accepteren van voorwaarden op televisie alvorens updatefunctie te gebruiken is.

[100] Ibid.

[101] Ibid.

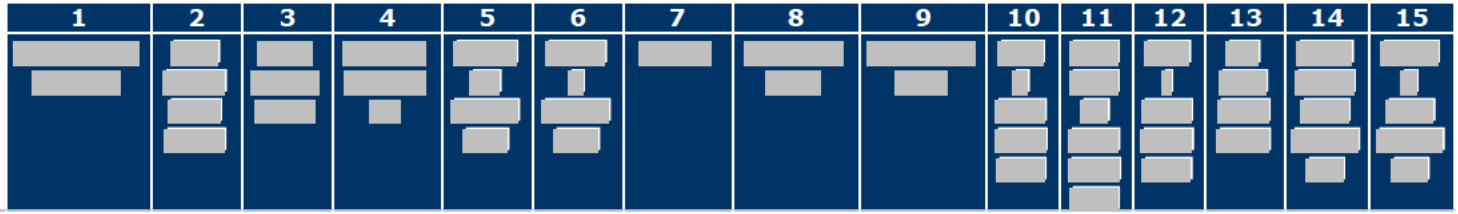
[102] Meting vanaf 8-4-2022.

[103] Versienummer niet beschikbaar.

[104] Meting vanaf 8-4-2022

[105] Ibid.

[106] Ibid.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
															
Aantal updates firmware 'hoofdapparaat' na ingebruikname	0	6	0	0	0	0	3	2	1	2	0	1	6	1	0
Minimumversie iOS gewijzigd sinds ingebruikname? (t/m 30-06-2022)	Nee (geen updates)	Nee	Nee	Nee	Ja (9.0 -> 10.0)	Nee	n.v.t.	n.v.t.	n.v.t.	Nee	Ja (iOS 12.0 -> 13.0)	Nee	Ja (iOS 11.0 -> 12.0)	Nee	Ja (iOS 13.0 -> 14.0)
Minimumversie Android gewijzigd sinds ingebruikname? (t/m 30-06-2022)	Nee (geen updates)	Nee	Ja (6.0 -> 8.0)	Ja (4.4 -> 5.0)	Nee	Ja (4.4 -> 5.0)	n.v.t.	n.v.t.	n.v.t.	Nee	Nee	Ja (6.0 -> 8.0)	Nee	Nee	Nee
Precontractueel verstrekte informatie															
Updatebeleid volgens verkoper	x	2 jaar	x	1 jaar	x	2 jaar	2 jaar	x	x	x	x	x	x	x	x
Updatebeleid volgens fabrikant	x	2 jaar	x	x	x	2 jaar	x	8 jaar	x	x	x	x	x	x	x
Minimumversie Android (smartphone) van bijbehorende app	Android 7.0	Android 7.0	x	x	x	x	n.v.t.	n.v.t.	n.v.t.	x	x	x	x	x	x
Minimumversie iOS/iPadOS van bijbehorende app	iOS 12.0	iOS 11.0	x	x	x	x	n.v.t.	n.v.t.	n.v.t.	x	x	x	x	x	x

Tabel 12 Overzicht van apparaten en FCIU-kenmerken waarvoor fabrikant en verkoper van elkaar verschillen in de precontractuele informatieverstrekking. Let op: bij de offline aankopen betreft het de online informatie verstrekt op de website van de verkoper. Een "x" geeft aan dat het betreffende kenmerk door ons niet is aangetroffen.

Apparaat ID	Korte naam apparaat	FCIU-kenmerk	Volgens informatie verkoper online bij aankoop	Volgens informatie fabrikant online op moment van aankoop
1	[redacted] lamp	Ondersteunde Wi-Fi-frequenties	2,4Ghz	x
1	[redacted] lamp	Internet nodig voor functies	Bediening via app	Installatie; Bediening kan zonder
1	[redacted] lamp	Ondersteunde smarthome-platformen, spraakassistenten	[redacted]	[redacted]
2	[redacted] lamp	Ondersteunde smarthome-platformen, spraakassistenten	[redacted]	[redacted]
2	[redacted] lamp	Minimumversie Android (smartphone) van bijbehorende app	Android 7.0	Android 8.0
2	[redacted] lamp	Internet nodig voor functies	Bediening via app	Installatie; Bediening kan zonder
2	[redacted] lamp	Minimumversie iOS/iPadOS van bijbehorende app	iOS 11.0	iOS 13.0
2	[redacted] lamp	Ondersteunt automatisch installeren van updates	x	Ja
3	[redacted] lamp	Minimumversie Android (smartphone) van bijbehorende app	x	Android 6.0
3	[redacted] lamp	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 14.0
3	[redacted] lamp	Internet nodig voor functies	x	Beperkte functionaliteit zonder
3	[redacted] lamp	Ondersteunt automatisch installeren van updates	x	Ja, verplicht om product te mogen gebruiken, kan in EU worden uitgeschakeld
4	[redacted] babyfoon	Gegarandeerde termijn voor volledige updates	1 Jaar	x
4	[redacted] babyfoon	Ondersteunde Wi-Fi-frequenties	2.4GHz	x
4	[redacted] babyfoon	Clouddienst nodig voor functies	Mogelijk	Delen met gezin
4	[redacted] babyfoon	Ondersteunde opslagmedia	SDXC	x
4	[redacted] babyfoon	Internet nodig voor functies	Werkt niet zonder Wifi	x

Apparaat ID	Korte naam apparaat	FCIU-kenmerk	Volgens informatie verkoper online bij aankoop	Volgens informatie fabrikant online op moment van aankoop
4	babyfoon	Minimumversie Android (smartphone) van bijbehorende app	x	Android 4.4
4	babyfoon	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 11.0
4	babyfoon	Ondersteunde smarthome-platformen, spraakassistenten	x	
5	babyfoon	Ondersteunde Wi-Fi-frequenties	2,4GHz	x
5	babyfoon	Clouddienst nodig voor functies	Mogelijk	Delen met gezin
5	babyfoon	Ondersteunde opslagmedia	SDXC	x
5	babyfoon	Internet nodig voor functies	Werkt niet zonder Wifi	x
5	babyfoon	Minimumversie Android (smartphone) van bijbehorende app	x	Android 5.0
5	babyfoon	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 9.0
6	babyfoon	Ondersteunde Wi-Fi-frequenties	2,4GHz; 5GHz	2,4Ghz
6	babyfoon	Minimumversie Android (smartphone) van bijbehorende app	x	Android 4.4
6	babyfoon	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 11.0
6	babyfoon	Clouddienst nodig voor functies	x	Betaalde dienst voor opslag
7	TV	Gegarandeerde termijn voor volledige updates	2 jaar	x
7	TV	Gegarandeerde termijn voor beveiligingsupdates	2 jaar	x
7	TV	Ondersteunde Wi-Fi-frequenties	2,4GHz; 5GHz	x
7	TV	Ondersteunde smarthome-platformen, spraakassistenten	x	
8	TV	Ondersteunde smarthome-platformen, spraakassistenten	Google Nest	x
8	TV	Internet nodig voor functies	Netflix, etc.	Instaleren van updates
8	TV	Gegarandeerde termijn voor volledige updates	x	8 jaar
8	TV	Gegarandeerde termijn voor beveiligingsupdates	x	8 jaar
8	TV	Ondersteunt automatisch installeren van updates	x	Ja
9	TV	Ondersteunde bedrade interfaces	Ja (o.a. HDMI 2.1, Ethernet RJ45, USB 3.2 Gen 1)	x

Apparaat ID	Korte naam apparaat	FCIU-kenmerk	Volgens informatie verkoper online bij aankoop	Volgens informatie fabrikant online op moment van aankoop
10	thermostaat	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 14.0
10	thermostaat	Clouddienst nodig voor functies	Cloudomgeving van de fabrikant nodig (gebruik zonder niet mogelijk)	x
10	thermostaat	Internet nodig voor functies	Alle	x
10	thermostaat	Compatibele 6LoWPAN-versie(s)	x	868MHz
11	thermostaat	Ondersteunde smarthome-platformen, spraakassistenten		
11	thermostaat	Ondersteunde bedrade interfaces	modulerende CV-ketel	Zowel aan/uit als OpenTherm
11	thermostaat	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 12.0
12	thermostaat	Ondersteunde bedrade interfaces	modulerende CV-ketel	Werkt met OpenTherm (Verwarming en warm water)
12	thermostaat	Ondersteunde Wi-Fi-beveiligingsmethoden	WEP	x
12	thermostaat	Ondersteunde Wi-Fi-technologieën	Wireless N	802.11b/g/n
12	thermostaat	Minimumversie Android (smartphone) van bijbehorende app	x	Android 6.0
12	thermostaat	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 14.0
12	thermostaat	Ondersteunt automatisch installeren van updates	x	Ja, verplicht om product te mogen gebruiken, kan in EU worden uitgeschakeld
13	wasmachine	Ondersteunde Wi-Fi-frequenties	2,4GHz	x
13	wasmachine	Minimumversie Android (smartphone) van bijbehorende app	x	Android 7.0
13	wasmachine	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 11.0
14	wasmachine	Internet nodig voor functies	Bediening via app	Voor specifieke functies: voor deze functie heb je een Wi-Fi-verbinding en een account nodig.
14	wasmachine	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 12.0 or later / iPhone 6 or later / iPad mini2 or later.

Apparaat ID	Korte naam apparaat	FCIU-kenmerk	Volgens informatie verkoper online bij aankoop	Volgens informatie fabrikant online op moment van aankoop
				Some mobile devices may not be supported
14	[redacted] wasmachine	Ondersteunde smarthome-platformen, spraakassistenten	x	[redacted]
14	[redacted] wasmachine	Clouddienst nodig voor functies	x	Voor specifieke functies: voor deze functie heb je een Wi-Fi-verbinding en een [redacted]-account nodig.
15	[redacted] wasmachine	Minimumversie Android (smartphone) van bijbehorende app	x	Android 6.0
15	[redacted] wasmachine	Minimumversie iOS/iPadOS van bijbehorende app	x	iOS 13.0
15	[redacted] wasmachine	Ondersteunde smarthome-platformen, spraakassistenten	x	[redacted]

[redacted]

Tabel 13 Updategeschiedenis apparaatsoftware per apparaat en daarbij gecontroleerde FCIU-kenmerken

Apparaat ID	Korte naam	Datum update	Versie apparaatsoftware na update	Wijzigingen geconstateerd voor FCIU-kenmerken?
2	[redacted] lamp	5-4-2022	[redacted]	Nee
2	[redacted] lamp	3-5-2022	[redacted]	Nee
2	[redacted] lamp	7-6-2022	[redacted]	Nee
2	[redacted] lamp	14-6-2022	[redacted]	Nee
2	[redacted] lamp	23-6-2022	[redacted]	Nee
2	[redacted] lamp	29-6-2022	[redacted]	Nee
7	[redacted] TV	30-3-2022	[redacted]	Nee
7	[redacted] TV	22-4-2022	[redacted]	Nee
7	[redacted] TV	20-6-2022	[redacted]	Nee
8	[redacted] TV	30-3-2022	[redacted]	Nee
8	[redacted] TV	31-3-2022	[redacted]	Nee
9	[redacted] TV	25-3-2022	[redacted]	Nee
10	[redacted] thermostaat	30-3-2022	[redacted]	Nee
10	[redacted] thermostaat	21-4-2022	[redacted]	Nee
12	[redacted] thermostaat	28-3-2022	[redacted]	Nee
13	[redacted] wasmachine	30-3-2022	[redacted]	Nee
13	[redacted] wasmachine	5-4-2022	[redacted]	Nee
13	[redacted] wasmachine	20-4-2022	[redacted]	Nee
13	[redacted] wasmachine	11-5-2022	[redacted]	Nee
13	[redacted] wasmachine	20-5-2022	[redacted]	Nee
13	[redacted] wasmachine	6-6-2022	[redacted]	Nee
14	[redacted] wasmachine	10-5-2022	[redacted]	Nee

Een overzicht van de onderzochte FCIU-kenmerken is te vinden in Tabel 1. In paragraaf 3.6 wordt toegelicht welke attributen na updates zijn gecontroleerd.

Bijlage 4. Resultatenmatrix digitale veiligheid

Deze bijlage is separaat beschikbaar als Excelbestand.

De uitkomsten van de tests van de digitale veiligheid van de apparaten zijn in detail beschreven in een resultatenmatrix. In deze matrix stellen de kolommen de apparaten voor (per testmoment is er een aparte kolom) en de rijen de geteste vereisten. In de cellen is de conclusie aangegeven:

- OK: apparaat voldoet aan het gestelde vereiste
- NA: het gestelde vereiste is niet van toepassing op het apparaat
- NT: het gestelde vereiste is niet te testen bij dit apparaat en/of gegeven de testopzet.
- W: het apparaat voldoet aan het vereiste, maar er is een aandachtspunt
- FAIL: het apparaat voldoet niet aan het gestelde vereiste.

Bij iedere conclusie is een korte toelichting gegeven. De vereisten zijn gegroepeerd naar Qbit- vereiste. In een aantal gevallen is het Qbit- vereiste rechtstreeks getest. In een aantal andere gevallen vormt een aantal IoTSF- vereiste gezamenlijk onderbouwing voor een Qbit- vereiste.

Bijlage 5. Kenmerken gebruikersapparaten

Gebruikersapparaat:	iOS	Android
Merk:	Apple	Motorola
Model:	iPad Air 2	Moto e20
Besturingssysteem:	iPadOS 15.0	Android 11 (RON31.267-22)
Modelnummer:	MNV22HC/A	XT2155-6
Serienummer:	DMPSQMCNHG5D	ZE22337KR5

Bijlage 6. Overige separate bijlagen

A. Details en gegevensarchief informatieverstrekking

Voorafgaand aan en tijdens de aankoop, en vervolgens wekelijks, is informatie opgehaald van een grote hoeveelheid webpagina's. Deze webpagina's zijn opgeslagen in verschillende formaten (de ruwe broncode, platte tekst en een schermafbeelding).

Het gehele archief is beschikbaar als Git-archief, waarmee eenvoudig vergelijkingen zijn te maken tussen verschillende versies. Hierbij is de gehanteerde lijst met URL's, alsmede de specifieke handelingen die nodig waren om de informatie op te halen (bijvoorbeeld het accepteren van cookies) beschikbaar.

B. Gegevens en verslagen aankopen

Van iedere aankoop zijn de factuur en eventuele andere relevante bestelgegevens beschikbaar. Van iedere offline aankoop is een verslag opgesteld, waarbij eveneens foto's zijn gemaakt van eventueel relevante productinformatie bij het apparaat.

C. Bewijsstukken analyse digitale veiligheid

Tijdens de analyse van digitale veiligheid is een dossier bijgehouden met 'bewijsstukken', bestaande uit schermafbeeldingen en output van de gehanteerde tools voor onder andere het scannen op zwakheden. Dit materiaal is gebundeld per apparaat beschikbaar.

D. Foto's verpakkingen en apparaten

Van alle apparaten en verpakkingen zijn foto's gemaakt. Deze foto's zijn per apparaat gebundeld beschikbaar.

E. Schermafbeeldingen ingebruikname

Tijdens de ingebruikname zijn van alle relevante stappen van ingebruikname van het apparaat (denk hierbij aan: gepresenteerde gebruiksvoorwaarden, het instellen van automatische updates, et cetera) schermafbeeldingen gemaakt. Deze schermafbeeldingen zijn gebundeld per apparaat beschikbaar.

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl