Handreiking Mobiele app Ontwikkeling en Beheer

voor de Nederlandse overheid

De Nederlandse overheid ontwikkelt steeds meer apps. Maar wat is nu een goede app? Waar moet je rekening mee houden? Welke standaarden zijn er? Deze gezamenlijke uitgave van Belastingdienst, DICTU, JIO , JIVC en SSC-I in samenwerking met provincies geeft hier antwoord op.

Finale versie 4.0

18 maart 2022

9 Colofon

Afzendgegevens	Coordinatie Handreiking: Belastingdienst – Mobile Competence Center John F. Kennedylaan 8, 7314PS Apeldoorn Postbus 950 7300 GM Apeldoorn mail naar: mcc.beheer@belastingdienst.nl		
Auteurs	Belastingdienst (Ministerie van Financiën) DICTU (Ministerie van Economische Zaken en Klimaat), SSC-ICT (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties) SSC-I DJI (Ministerie van Justitie en Veiligheid) JIVC (Ministerie van Defensie) Politie (review)		
Versiebeheer	1.0	Maart 2017	Definitieve versie, geaccordeerd in CTO-Raad Rijk
	2.0	Mei 2018	Definitieve versie, geaccordeerd in CTO-Raad Rijk
	3.0	Mrt 2020	Voorzien van updates en aanpassingen
	4.0	Mrt 2022	Voorzien van updates en aanpassingen

Inhoud

10 Inleiding

Doelstelling

De Handreiking Mobiele App Ontwikkeling en Beheer voor de Nederlandse overheid draagt bij aan een eenduidige uitstraling, beveiliging en werking van apps van en voor de overheid. Dit document heeft als doel dat organisaties die voor en namens de overheid apps ontwikkelen gebruik maken van elkaars kennis en ervaring. Deze handreiking omvat een breed scala aan onderwerpen die generiek zijn voor de ontwikkeling en beheer van apps van en voor de overheid; dit kunnen zowel apps voor de medewerkers van de Nederlandse overheid zijn, als apps voor burgers en bedrijven.

Wat is een App?

Een app is meer dan een afkorting van “applicatie”.
Een app richt zich idealiter op de realisatie van één of meer functionaliteiten. Dit document richt zich op apps voor mobiele devices (tablets en smartphones en “wearable” devices) en hybride devices (laptops met een los koppelbaar toetsenbord en aanraakscherm). Apps voor niet-mobiele devices en onderwerpen gerelateerd aan het “Internet of Things” laten we in deze versie buiten beschouwing omdat de architectuur hiervan volledig afwijkt van die van apps.

Doelgroep

Dit document is bedoeld voor organisaties die apps (laten) ontwikkelen voor het Rijk, Provincies en Gemeenten. Het is zowel technisch als beleidsmatig van aard en gericht op opdrachtgevers, ontwerpers, architecten en ontwikkelaars. Dit document beoogt in de breedte compleet te zijn voor het onderwerp app ontwikkeling en beheer voor de benoemde doelgroepen. Wanneer onderwerpen ergens anders beschreven zijn, wordt daarnaar verwezen via hyperlinks.

Totstandkoming en borging

Deze handreiking is tot stand gekomen in opdracht van de CTO-Raad Rijk aan Belastingdienst, DICTU (Ministerie van Economische Zaken en Klimaat), SSC-ICT (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties) en SSC-I (Ministerie van Justitie en Veiligheid). De inhoud is breed getoetst door partijen binnen de (Rijks)overheid die apps ontwikkelen of daartoe opdracht geven. Dit document is opgenomen in de Enterprise Architectuur Rijk (EAR). De verantwoordelijkheid voor het beheer van dit document ligt bij toerbeurt bij een van de partijen betrokken bij het schrijven van dit document. Jaarlijks kijken we daarbij naar ontwikkelingen in ons vakgebied die al naar gelang de impact opgenomen of aangepast kunnen worden in dit document.

1 Beleid

Het is vanzelfsprekend dat apps van de overheid voldoen aan het beleid, standaarden en architectuurkaders van diezelfde overheid. Tegelijkertijd moeten apps (zo veel als mogelijk) voldoen aan standaarden die binnen de mobiele wereld gangbaar zijn.

1.1 Beleid en overheidsstandaarden

Binnen het Rijk is de I-Strategie van het Rijk 2021 -2025: vigerend[1]".

De Open standaarden van het Forum Standaardisatie[2] en de diverse architectuur standaarden van de overheid (zoals bv. de EAR standaarden[3] voor de Rijksoverheid) gelden voor alle aspecten van de voorzieningen van de (Rijks)overheid en daarmee ook voor de dienstverlening via apps. Het voorbeeld van een technische referentie architectuur voor app ontwikkeling is de "Referentie architectuur voor mobiele applicaties"[4] van DICTU.

- Voldoe aan de kaders van de overheid.
- Sluit zo veel mogelijk aan op de gangbare publieke (open) standaarden
- Principes als Tijd, Plaats en Apparaat onafhankelijk Werken (TPAW), "De gebruiker staat centraal", loosely coupled architectuur en beveiligingsbewustzijn, zijn leidend.

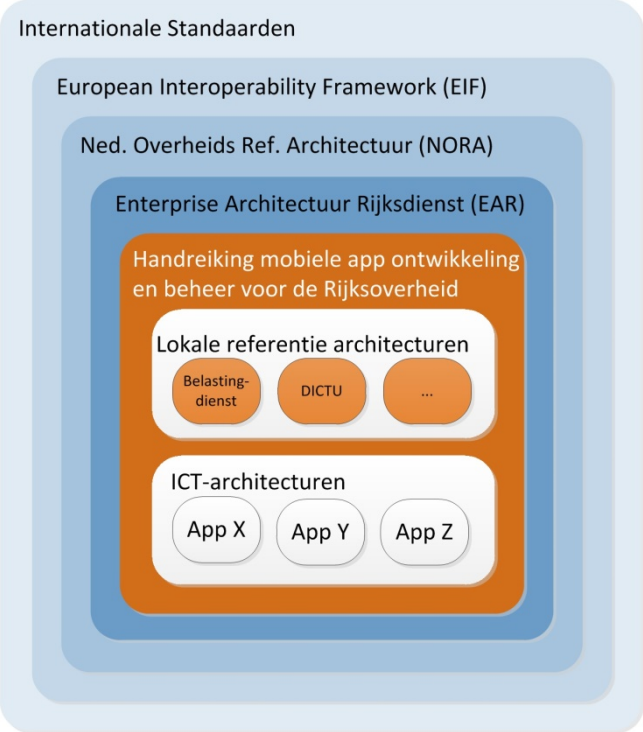
1.2 Publieke standaarden

Vanwege het dynamische karakter van de mobiele wereld is het raadzaam om de (open) standaarden van de private sector, zoals leveranciers, zo veel als mogelijk te gebruiken.

[1] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/i-strategie-rijk-2021-2025/
[2] https://www.forumstandaardisatie.nl/open-standaarden
[3] https://www.earonline.nl/index.php/Overzicht_standaarden
[4] Op te vragen via w.j.r.heukers@dictu.nl

1.3 Architectuurkaders

Deze Handreiking Mobiele App Ontwikkeling en Beheer voor de (Rijks)overheid kan beschouwd worden als een te realiseren doelarchitectuur van de Enterprise architectuur Rijksdienst (EAR)[5]. De EAR conformeert aan de Nederlandse overheid Referentie Architectuur (NORA)[6] die weer binnen het (European Interoperability Framework (EIF))[7] valt.



1.4 Principes

Principes zijn een deel van het instrumentarium van iedere architectuur en zijn richtinggevend voor het nemen van besluiten en/of uitgangspunt voor acties. De hieronder genoemde principes voor ontwikkeling van apps zijn afgeleid van de EAR en van best practices uit de mobiele wereld.

Bevorder Tijd, Plaats en Apparaat onafhankelijk Werken (TPAW). Iedereen kan zijn of haar werkzaamheden onafhankelijk van tijd, plaats en apparaat uitvoeren, volgens het EAR principe: "Altijd, overal, ieder apparaat[8]". (Zie ook: WPD: Plaats- Tijd- Organisatie- Apparatuuronafhankelijk - EAR Online). Dit geldt zowel voor beleids- als uitvoeringsfuncties. Het TPAW principe beperkt zich niet tot het werken op een vaste werkplek. De moderne tijd en de komst van het hybride werken, vereisen eigenlijk dat men overal kan werken: thuis, onderweg, op de locatie van een ketenpartner of bij een specifieke doelgroep.

Voldoende veilig. Mobiel werken brengt veiligheidsrisico's met zich mee, bijvoorbeeld doordat bij verlies of diefstal gegevens gemakkelijk "op straat" terecht kunnen komen. Hoe veilig een app moet zijn, is afhankelijk van de toepassing van de app en de classificatie van de data in de app. Het hoofdstuk 'Informatiearchitectuur' werkt dit verder uit. De juiste set van beveiligingsmaatregelen wordt bepaald via een risicoanalyse. In het hoofdstuk 'Beveiliging' wordt dit verder uitgewerkt.

Respecteer privacy betrokkenen. Deze wordt deels vanuit wetgeving zoals de AVG afgedwongen. Privacy omvat o.a. het voldoende beschermen van de gegevens die je in een app verzamelt, verwerkt

[5] http://www.earonline.nl/index.php/Welkom_op_de_kennisbank_van_de_Enterprise_Architectuur_Rijksdienst
[6] http://www.noraonline.nl/wiki/NORA_online
[7] https://ec.europa.eu/isa2/eif_en
[8] http://earonline.nl/index.php/Informatiseringsdomein_Werkplekdiensten

of bewaart. De maatregelen die bij ‘voldoende veilig’ zijn geindentificeeerd helpen hier in belangrijke mate bij. Maar privacy is meer; het behelst ook transparantie over wat de aanbieder van de app met die gegevens doet, het niet langer bewaren van gegevens dan strikt noodzakelijk en het faciliteren in de rechten van betrokkenen (denk aan inzage en correctie) m.b.t deze verwerkingen.

Hergebruik van bouwstenen, zoals beschreven in het EAR-principe hergebruik bouwstenen,[9] bevordert in veel gevallen de efficiency bij ontwikkeling, onderhoud en het beheer. Hergebruik moet echter genuanceerd worden toegepast, het kan namelijk ook tot kosten-inefficiëntie leiden.

Het **loosely coupled** interacteren (met name met middle tiers en back ends) verhoogt de beheersbaarheid en onderhoudbaarheid van een oplossing.

De gebruiker staat centraal. In de mobiele context draait het, nog meer dan bij de ontwikkeling van reguliere software, om de gebruikerservaring. In de hoofdstukken ‘Bedrijfsarchitectuur’ en ‘User epxerience’ wordt dit principe uitgewerkt. Bij mobiele apps kan er een *trade off* tussen veiligheid en user experience ontstaan.

De app heeft **toegevoegde waarde** voor de organisatie, maar ook voor de gebruiker.

[9] http://earonline.nl/index.php/Afspraak_-_Gebruik_beschikbare_bouwstenen

2. Bedrijfsarchitectuur

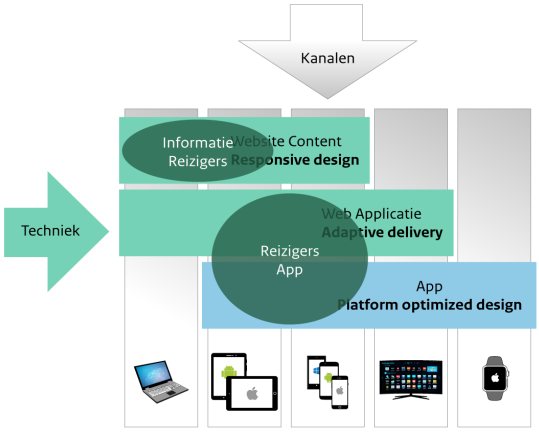
Smartphones, wearables en tablets worden vaker en langduriger gebruikt dan computers en laptops. Voor regelmatig terugkerende taken worden vaker apps gebruikt dan websites.[10] Voor de overheid is het dus van belang om burgers en bedrijven mobiel te ondersteunen en apps te ontwikkelen.

2.1 Toegevoegde waarde bedrijfsstrategie

Een app moet ten opzichte van de traditionele applicaties of websites toegevoegde waarde leveren die past binnen de bedrijfsstrategie. Het gebruik van een app verhoogt bijvoorbeeld de efficiëntie van de uitvoering van een bedrijfsproces. Apps verhogen de zichtbaarheid van een ministerie of een dienst naar buiten. Op basis van de eigenschappen en behoeften van de gebruiker bepaalt de organisatie welke diensten mobiel aangeboden worden. De IT-afdeling helpt daarnaast de gebruikers inzicht te krijgen in de nieuwste technieken en functionele mogelijkheden, die kunnen leiden tot bijgestelde of nieuwe behoeften.

- Gebruik apps voor snellere en betere interactie met de gebruiker binnen de bedrijfsstrategie.
- Zorg voor aansluiting van de app op het doel, de doelgroep en de eindgebruiker.
- Laat de app passen in de device- strategie.
- Zorg voor transparantie in het gebruik van informatie door de app.
- Een app is pas een succes als deze gebruikt wordt.

Voor mobiele toepassingen is de interactie met gebruikers hoger dan bij traditionele omgevingen. Voor de aanbieder van de app is het eenvoudiger om de gebruiker te bereiken via bijvoorbeeld push-notificaties. Het beste is om daar ook meteen een goed handelingsperspectief aan te bieden, zodat de gebruiker direct iets kan afhandelen. Een belangrijke drempelverlagende eigenschap is dat apps vaak een sterke maar niettemin gebruikersvriendelijke authenticatie bieden om de gewenste handeling snel en veilig uit te voeren. Daarnaast biedt een mobiel device toegang tot persoonlijke data, zoals agenda en contacten en beschikt deze over een scala aan sensoren.



[10] bronnen: o.a. Flurry, Comscore

2.2 Aansluiting op de eindgebruiker

Gebruikers zijn gewend aan een groot aanbod van kwalitatief goede apps vanuit de publieke app stores. Het “responsive maken” van websites of applicaties is een mogelijke stap om de mobiele gebruiker te bereiken. Dit levert echter niet altijd het gewenste resultaat op. Onderzoek daarom bij het aanbieden van mobiele diensten hoe de gebruiker optimaal ondersteund kan worden. Houd hierbij rekening met factoren als tijdstip, locatie, activiteit, hoeveelheid informatie die getoond wordt op het scherm, hoeveelheid invoer via toetsenbord en mate van interactiviteit. Op basis hiervan kan een keuze gemaakt worden op welke wijze een dienst beschikbaar gemaakt wordt. Deze keuze hoeft niet altijd een eenduidige oplossing te zijn, maar kan ook betekenen dat de dienst op meerdere kanalen aangeboden wordt. Bijvoorbeeld niet alleen een app, maar ook een website.

2.3 Doel en doelgroep

Apps zijn anders dan traditionele applicaties. Apps zijn bedoeld voor het uitvoeren van een bepaalde taak of aan elkaar gerelateerde taken. Voorkomen moet worden dat een app te veel (ongebruikte) functionaliteit in zich heeft en hierdoor complex en moeilijk in gebruik wordt. Tegelijkertijd is het niet gewenst om burgers en bedrijven te overspoelen met grote aantallen apps die één specifieke taak uitvoeren. Onderken daarom de doelgroepen voor een app en bied per doelgroep één app aan met alle relevante functionaliteiten. Bijvoorbeeld een app voor burgers en een app voor bedrijven om te communiceren met de organisatie. Hetzelfde geldt voor interne apps. Niet elke medewerker heeft elke app van de organisatie nodig en ook is het niet wenselijk om één app per organisatie te maken vanwege de afhankelijkheden en autorisaties die gemanaged moeten worden. Voor apps die een primair proces ondersteunen is een goede richtlijn om alle mobiel uit te voeren taken van het betreffende proces in één app te integreren. Dit kan betekenen dat sommige functies in meerdere apps terugkomen. Een voorbeeld hiervan is een functie voor het opvragen van informatie over een voertuig op basis van een kenteken. Deze functie wordt gebruikt bij het proces voor toezicht op betaling van motorrijtuigenbelasting, maar ook voor het proces van een deurwaarder voor beslaglegging. In beide gevallen is de informatie ook nodig in het verdere proces en daarom is de functie volledig geïntegreerd.

2.4 Device-strategie

De app houdt rekening met de device-strategie die binnen de organisatie wordt gehanteerd, denk hierbij aan de platformkeuzes, Bring Your Own Device (BYOD)-beleid, autorisatiemogelijkheden en wijze van distributie. Apps voor burgers en bedrijven kennen een diversiteit aan mogelijke platformen (Android, iOS, etc.) en worden gedistribueerd via publieke app stores. Het platform van de app van de medewerker is over het algemeen bekend omdat de mobiele devices vaak door de organisatie worden uitgegeven. Apps voor gebruikers die voor de overheid werken worden gedistribueerd via een UEM (Unified Endpoint Management) oplossing, via enterprise app stores of middels custom app publicatie

in de iOS en Android stores. In het hoofdstuk ‘Beheer en distributie’ wordt aandacht besteed aan de distributie van apps.

Veel organisaties bieden medewerkers de mogelijkheid om hun privé-device te gebruiken voor zakelijke toepassingen (BYOD). Vaak zullen naast bedrijfsdevices dus ook privé-devices door een EMM-oplossing beheerd worden. Dit is nodig voor toegang tot diensten en beveiliging van informatie. Voor goede BYOD-ondersteuning is het noodzakelijk om een aantal beslissingen te nemen en deze ook helder te communiceren zoals:

1. Welke werkzaamheden voor de organisatie op een privé-device uitgevoerd mogen worden. Is dit beperkt tot E-mail en social apps of is het ook gewenst om primaire processen met gevoelige informatie te ondersteunen op BYOD en wat zijn de beveiligingseisen daarvoor (zie hoofdstuk ‘Beveiliging’).
2. Welke platformen en versies (Android, iOS, etc.) voor privé-devices worden ondersteund. Dit zal vaak bepaald worden door de ondersteuning van de EMM leverancier, Wifi bedrijfsnetwerk, E-mail en samenwerking-platform ondersteuning.
3. Privacy-aspecten van het gebruik van eigen apparatuur. Welke informatie van het apparaat of de gebruiker wordt door de organisatie verzameld, verwerkt en opgeslagen. Wat wordt met deze informatie gedaan.

2.5 Transparantie

Mobiele devices bieden veel mogelijkheden en bevatten veel persoonlijke data. De app moet de gebruiker duidelijk maken hoe hiermee wordt omgegaan. De bestaande platformen gaan steeds verder in het beschermen van privacygevoelige data voor hun gebruikers. De nieuwste versies van iOS en Android bijvoorbeeld, zorgen ervoor dat de gebruiker altijd toestemming moet geven voor het gebruik van GPS, camera, toegang tot contacten of de agenda. Hierbij moet de app aangeven wat de reden is voor toegang. Net als websites maken apps ook gebruik van het verzamelen van statistieken. En net als bij websites is het belangrijk dat de gebruiker geïnformeerd wordt en *in control* is zodat er geen misbruik gemaakt kan worden door analytics diensten. De verzamelde data kunnen bijvoorbeeld gebruikt worden voor het opbouwen van profielen.

2.6 Succesvolle apps

Tenslotte, het succes van een app ligt ook in het daadwerkelijke gebruik ervan. Zorg dus voor goede communicatie en/of marketing voor de app en het daarvoor benodige budget. Voor publieke apps kunnen hiervoor advertenties en social media worden ingezet. Gebruik voor interne apps een bericht op intranet, interne social media of de klassieke posters ”in de lift”. Monitor het gebruik van de app en breng regelmatig updates met verbeteringen en/of nieuwe functionaliteiten uit. Het vasthouden van het succes vraagt om pro-actief eigenaarschap en beheer van een app.

3. Informatiearchitectuur

De aard van de informatie die in een app komt te staan, is van invloed op de ontwikkeling van een app. Mobiele devices bieden meer mogelijkheden in het aanbieden van informatie, zoals bijvoorbeeld locatiegegevens en er zijn maatregelen nodig om deze informatie te beschermen.

Afhankelijk van de informatie die een app bevat, moeten bepaalde beveiligingsmaatregelen worden genomen. Deze maatregelen worden bepaald op basis van de waarde van de informatie voor de organisatie of de gebruiker van de app.

- Classificeer de informatie die in de app komt te staan.
- De mogelijkheden van een device kunnen bepalen hoe informatie wordt vastgelegd.
- Sla informatie lokaal op met passende maatregelen.
- Combineer informatie uit verschillende bronnen in een app.
- Verrijk de echte wereld met digitale informatie.

3.1 Classificatie

Door een classificatie van de informatie toe te passen is het mogelijk om standaard maatregelen te definiëren per classificatie. De Algemene Verordening Gegevensbescherming (AVG) is hierbij een uitgangspunt. De AVG gaat over gegevens m.b.t. individuen, maar ook andere gegevens kunnen belangrijk zijn voor een organisatie. Binnen de diverse lagen van de overheid zijn hier reeds rubriceringsvoorschriften voor zoals bij het Rijk het VIR en VIR/BI (Voorschrift Informatiebeveiliging Rijksdienst / Bijzondere Informatie)[11].

De classificering van informatie in apps voor medewerkers kan het beste gebeuren met de bestaande methode binnen de eigen organisatie. Onderstaande figuur bevat een voorbeeld van de verschillende classificatie niveaus.

Niveau	Classificatie informatie publieke apps	Classificatie informatie interne apps
Laag	Publieke informatie	Publieke informatie of Open Data
Midden	Persoonsgegevens	Departementaal Vertrouwelijk
Hoog	Bijzondere persoonsgegevens of financiële gegevens	Departementaal Vertrouwelijk met een hoger dan gemiddeld dreigingsniveau of Staatsgeheim/ Confidentieel

[11] https://wetten.overheid.nl/BWBR0033507/2013-06-01

3.2 Privacybeginselen

Sinds 25 mei 2018 is de AVG van kracht. Hierin wordt gereguleerd hoe een organisatie dient om te gaan met de verwerking van gegevens over personen. De AVG is gebaseerd op een aantal belangrijke principes. In de informatie-architectuur dienen deze terug te komen. Een aantal van deze principes zijn:

1. Doelbinding; de gegevens worden slechts vastgelegd en gebruikt voor het doel waarvoor de app ontwikkeld wordt.
2. Legitimiteit en transparantie; het doel waarvoor de app en de gegevens worden gebruikt past binnen de doelstellingen van de organisatie. De organisatie moet o.a. kunnen uitleggen wat het doel is, waarom dit doel legitiem is, en welke gegevens worden verwerkt, wie er toegang toe heeft en met wie ze gedeeld kunnen worden.
3. Proportionaliteit en subsidiariteit; het proportionaliteitsvereiste brengt met zich dat het doel van de verwerking van de persoonsgegevens in verhouding moet staan tot de inbreuk op de privacy van de betrokkene. Het subsidiariteitvereiste houdt in dat onderzocht moet worden of het doel ook op een andere wijze kan worden bereikt, waarbij de inbreuk op de privacy van de betrokkene minder is. De betrokkene is de persoon van wie de gegevens in de app en/of het achterliggende systeem worden vastgelegd of verwerkt.
4. Gegevensminimalisatie; er moeten niet meer gegevens verzameld worden dan strikt nodig is voor de aangegeven doelen.
5. Bewaar niet langer dan nodig; bij het bepalen van welke gegevens er benodigd zijn, dient ook vastgesteld te worden hoe lang deze gegevens bewaard mogen worden. Het uitgangspunt is hier niet langer dan nodig. Voor sommige informatie geldt een archief- of bewaarplicht. In dat geval gelden er behalve maximale bewaartermijnen ook minimale termijnen.
6. Accuraatheid; de gebruiker dient er op te kunnen vertrouwen dat de gegevens zoals deze gepresenteerd en vastgelegd worden correct zijn en blijven gedurende de tijd dat deze worden bewaard.
7. Vertrouwelijkheid; hoe hoger de classificatie van persoongegevens, des te hoger de eisen die aan vertrouwelijkheid worden gesteld. Deze eisen gelden voor de techniek (denk aan encryptie van de gegevens), maar ook voor het personeel en de processen binnen de verwerkende organisatie.
8. Verantwoording en rechten van betrokkene; het moet voor de betrokkene inzichtelijk zijn welke acties er met zijn gegevens zijn gedaan. Bijvoorbeeld: welke mutaties hebben er plaatsgevonden, wie heeft inzage gehad? Daarnaast heeft een betrokkene het recht om zijn gegevens in te kunnen zien, te laten muteren en te laten verwijderen (mits toegestaan binnen wettelijke kaders).

3.3 Vastleggen van informatie

Mobiele devices beschikken over sensoren die mogelijkheden bieden om informatie op een andere manier te vergaren dan alleen de traditionele tekstinvoer. Daarnaast bieden platformen een breed scala aan mogelijkheden om informatie aan de gebruiker te kunnen aanbieden op andere manieren dan in de app zelf.

Invoeren van informatie. Bij het invoeren van informatie is het belangrijk om te bepalen wat de mogelijkheden zijn die standaard geboden worden door de devices. Er zijn twee belangrijke redenen om dit te doen:

- Eenvoudigere invoer. De meeste mobiele devices zijn niet ontworpen om veel tekst in te voeren via een toetsenbord;
- Nauwkeurigheid verhogen. Door gebruik te maken van sensoren kun je meer of gedetailleerdere informatie vergaren dan via traditionele tekstinvoer.

Het maken van een foto in plaats van het vragen van een uitgebreide omschrijving biedt niet alleen een gedetailleerde vastlegging ,maar ook een veel betere gebruikerservaring. Ook kan een foto eventueel aangevuld worden met extra informatie. Een ander voorbeeld is het vastleggen van een locatie via de GPS-sensor van een device door middel van coördinaten in plaats van een adres. Veel platformen bieden ook de mogelijkheid om een vertaling te maken van coördinaten naar adresgegevens en omgekeerd, om uiteindelijk eenvoudig de gewenste informatie te verkrijgen.

Aangezien de data van sensoren als de camera of GPS ook misbruikt kunnen worden, schermen de meeste platformen het gebruik ervan af. Pas na toestemming van de gebruiker zal de app toegang krijgen tot de sensoren. Zorg in de app dus voor een heldere uitleg waarom en waarvoor de informatie van de betreffende sensor nodig is. Dit wordt ook steeds vaker vereist vanuit de platformleveranciers.

Aanbieden van informatie. Informatie kan in de app zelf worden getoond, maar ook zonder de app te openen in de vorm van een notificatie, een widget op een startscherm, via personal assistants (Siri, Google Assistent, enz.) of zoekfaciliteiten van het platform. Informatie van buiten de app is eenvoudiger toegankelijk voor de gebruiker en deze kan ook vaak nog een bewerking door de platformleverancier ondergaan. Publieke informatie kan zonder problemen buiten de app worden aangeboden. Als het echter over persoonsgegevens of vertrouwelijke informatie gaat, is het goed om een afweging te maken tussen gebruikerservaring en privacy/beveiliging.

3.4 Lokaal opslaan

Mobiele devices bieden apps de mogelijkheid om informatie lokaal op het device zelf op te slaan. Dit kan nodig zijn voor een betere gebruikerservaring, voor een lagere belasting van de backend (de systemen waar de app informatie uit haalt) of voor offline gebruik van de app. Aangezien mobiele devices gevoeliger zijn voor verlies of diefstal, is het belangrijk om de informatie die lokaal opgeslagen is op een goede, passende manier te beveiligen. Meer informatie over beveiliging van apps is te vinden in het hoofdstuk ‘Beveiliging’. Zwaarwegende redenen om lokaal informatie op te slaan zijn:

- **Gebruikerservaring.** Gebruikers zijn gewend dat apps snel reageren. Dit betekent dat informatie die getoond wordt, snel beschikbaar moet zijn. Het tijdelijk opslaan (cachen) van gegevens op het device kan ervoor zorgen dat informatie direct beschikbaar is en er niet gewacht hoeft te worden tot de informatie vanuit het datacenter beschikbaar is. Een

voorbeeld hiervan zijn E-mail-applicaties waarbij E-mails lokaal opgeslagen worden en deze direct bij opstarten al getoond worden.

- **Belasting van de backend.** Door lokaal data op te slaan kan het aantal vragen naar de backend beperkt worden. Denk hierbij aan lokaal opslaan van statische data die in een app gebruikt wordt (cf. lijsten met organisatieonderdelen, landen en regio's).
- **Offline gebruik.** Op sommige locaties is de beschikbaarheid van een verbinding met Internet niet gegarandeerd. Als de app dan ook gebruikt moet kunnen worden, dient data lokaal opgeslagen te worden. Dit geldt ook voor de ingevoerde data die dan op een later moment verzonden wordt. Een voorbeeld is de Fysiek Toezicht app van de Douane waarmee medewerkers controles uitvoeren, op de locatie waar geen connectie beschikbaar is.

3.5 Combineren van bronnen

Aangezien apps ook informatie buiten het bedrijfsnetwerk kunnen benaderen, is het combineren van informatie van buitenaf met informatie van het interne netwerk een belangrijke mogelijkheid van apps. Door het combineren van informatie kan de dienstverlening verbeterd worden en vaak ook aansluiten op een persoonlijke situatie. Een aantal voorbeelden is hier toegelicht.

Open data. De overheid heeft een ruim aanbod van open data datasets[12]. Deze data combineren met de informatie van de gebruiker of de eigen organisatie kan een verrijking betekenen voor de gebruiker. Een voorbeeld is een medische app die gebruik maakt van open data sets met de actuele luchtkwaliteitsindex en fijnstofconcentratie.

Social Media. Vanuit apps is het mogelijk om snel en eenvoudig te integreren met de mogelijkheden van social media. Via een AMBER Alert app bijvoorbeeld, kan de gebruiker een melding delen op bijvoorbeeld Facebook of Twitter. Een andere toepassing is het gebruik van profielinformatie vanuit social media. Het is hierbij wel belangrijk om rekening te houden met privacy-aspecten en te voorkomen dat geclassificeerde bedrijfsinformatie naar buiten lekt. Een goede voorlichting voor medewerkers is hierbij noodzakelijk.

Kaarten. Vanuit de platformen worden kaartvoorzieningen aangeboden om informatie op een kaart te visualiseren. Deze kaarten bieden steeds meer mogelijkheden om additionele informatie te integreren, bijvoorbeeld verkeersinformatie of locaties van instellingen. Belangrijk bij het gebruik van kaarten is de privacy in de gaten te houden, immers de kaart die opgevraagd wordt bij het platform, kan gebruikt worden om een profiel te verrijken. De

[12] https://data.overheid.nl/

voorziening Publieke Dienstverlening Op de Kaart (PDOK)[13] van de Nederlandse overheid heeft dit risico niet, het hoofdstuk 'Geografische functionaliteit' gaat hier verder op in.

Agenda, Contacten. Mobiele devices hebben standaard voorzieningen voor email, agenda en contacten en bieden de mogelijkheid om deze te gebruiken in apps. Een voorbeeld hiervan is de BTW Alert app waarbij herinneringen in de agenda van de gebruiker worden geplaatst voor een tijdige aangifte van BTW. Om toegang te krijgen tot de persoonlijke agenda of de contacten moet de gebruiker toestemming geven, zorg dus voor transparantie in de app over het gebruik van deze gegevens.

3.6 Virtual reality, augmented reality en machine learning

Tenslotte, maak gebruik van informatie uit de virtuele wereld om de werkelijkheid te verrijken. Doordat mobiele devices steeds meer rekenkracht krijgen en beschikken over een breed scala aan sensoren, is er steeds meer mogelijk. Denk aan het tonen van informatie door middel van een mobiel device of een virtual reality (VR) bril om inzicht te geven in een toekomstige situatie of voor trainingstoepassingen. Via augmented reality (AR) wordt de echte wereld getoond in het scherm van een mobiel device en - soms levensecht - verrijkt met virtuele informatie. De inzet van machine learning waarbij via modellen en algoritmen artificiële intelligentie toegepast kan worden op de informatie uit de sensoren, biedt mogelijkheden zoals het herkennen van objecten in foto's en het begrijpen van gesproken tekst. Machine learning voor objectherkenning kan in combinatie met AR heel krachtig zijn voor het realtime tonen van informatie in een blik op de echte wereld, bijvoorbeeld door op een auto informatie van de eigenaar te projecteren op basis van het kenteken van de auto.

[13] https://www.pdok.nl/

4. Standaard Pakketten

4.1 Inkoop

- Vergeet de mobiele component niet bij de uitvraag voor standaard pakketten.
- Mobiele apps van standaard pakketten dienen up-to-date gehouden te worden met de operating systemen.
- Zorg in een uitvraag dat de overheidseisen op gebied van de beveiliging, privacy en toegangelijkheid worden meegenomen.

Neem het mobiele gebruik van een ICT-oplossing ook mee bij de aanschaf van een ICT-systeem. Goede mobiele ondersteuning kan de effectiviteit van een ICT-oplossing verhogen. Niet alleen voor medewerkers op locatie maar ook voor office-werkers die middels hun smartphone vaak sneller en effecienter kunnen handelen waardoor processen sneller verlopen. Mobiele ondersteuning kan middels apps of mobiele web-applicaties. Zorg dat kosten van het mobiele gebruik ook inzichtelijk zijn. Vaak zal extra betaald moeten worden voor een app. Of als er een API beschikbaar is voor een eigen app zal hiervoor ook betaald moeten worden. Vergeet deze aspecten niet in een marktuitvraag.

4.2 Eisen aan ondersteuning

Web-applicaties. Voor mobiele web-applicaties is het verstandig om ondersteuning en updates te eisen zodat de web-app goed werkt in de browser van de EMM-leverancier. Door deze browser te gebruiken kan er een veilige verbinding met de systemen intern gemaakt worden. Let op, deze browsers zijn vaak minder rijk dan de reguliere browsers dus compatibiliteit, goede performance en ondersteuning eisen in een uitvraag voorkomt een hoop problemen.

Apps. Bij apps is er nog meer aandacht nodig voor de eisen die gesteld moeten worden aan de ondersteuning. Zo moeten apps up-to-date gehouden worden om te blijven functioneren. De updates van mobiele operating systemen zijn daarbij een belangrijk aandachtspunt. Zo is het belangrijk om te eisen dat de apps blijven functioneren bij updates van het operating systeem. De distributie van enterprise apps vraagt ook aandacht, zorg dat de leverancier de app op de juiste manier blijft aanbieden conform de eisen die Apple en Google stellen aan de distributie. Let op, afhankelijk van de doelgroep kan de distributie anders zijn (zie hoofdstuk 11). Neem dit ook mee in een uitvraag. Om optimaal aan te sluiten op de eigen EMM-oplossing en een vendor-lock-in te voorkomen op de EMM-oplossing is het raadzaam om voor enterprise integratie te eisen dat deze voldoet aan app.config (zie hoofdstuk 7).

4.3 Technische aandachtspunten

Als een leverancier zelf geen mobiele oplossing biedt of de oplossing voldoet niet, dan is het belangrijk om in de uitvraag een API te eisen die de benodigde functies voor een mobiele oplossing ontsluit. Het is dan namelijk mogelijk om zelf een mobiele oplossing te maken die aansluit op deze API. Dergelijke maatwerk apps kunnen binnen de Rijksoverheid door bijvoorbeeld het Dictu AppLoket, het Mobile Competence Center van de Belastingdienst of de markt worden gerealiseerd. Voor mobiele apps kan het belangrijk zijn om notificaties te gebruiken. Bij SAAS oplossingen is dit meestal makkelijk geregeld maar dient wel gecontroleerd te worden of er geen datalekken zijn omdat third-party notificatie-diensten gebruikt worden. Bij on-premise ICT-systemen is het verstandig met de ICT-afdeling af te stemmen hoe push notificaties ondersteund kunnen worden. Met name netwerkbeveiliging is een aandachtspunt.

4.4 Wettelijke eisen

Beveiliging. Het maken van veilige apps die door de overheid gebruikt worden vraagt meestal wat extra van de leverancier. Zo is het belangrijk om de authenticatie te kunnen koppelen aan de eigen systemen. Dit kan middels SAML, OAuth of ondersteuning van SSO dat aangeboden wordt door de eigen EMM-oplossing. Ook dient afhankelijk van de data classificatie de opgeslagen data afdoende beveiligd te zijn. Dit kan betekenen dat er naast de versleuteling van het operating systeem soms nog een extra versleuteling vereist kan zijn. Neem de juiste beveiligingseisen mee in een uitvraag (zie hoofdstuk 10).

Privacy. Bij een app dient de dataverwerking, logging en analytics te voldoen aan de wettelijke eisen op gebied van privacy. Neem deze, bv. AVG, mee in een uitvraag (zie hoofdstuk 3).

Toegangelijkheid. Mobiele oplossingen die binnen de overheid worden aangeboden aan medewerkers dienen te voldoen aan de WCAG regels. Zorg dat leverancier een onafhankelijk toets heeft laten uitvoeren om vast te stellen dat de app hieraan ook daadwerkelijk voldoet (zie hoofdstuk 8).

5. Softwarearchitectuur

De softwarearchitectuur voor apps kent in het algemeen een grote diversiteit. Er zijn native apps, cross platform apps, hybride apps en web apps en er zijn diverse platformen en versies waarvoor ontwikkeld kan worden. Ook komen specifieke mobiele onderwerpen zoals push-notificaties en geografische functionaliteit aan bod. In de huidige versie van dit document gaan we uit van iOS en Android als de belangrijkste mobiele platformen. Het advies is wel om de ontwikkeling van Harmony OS door Huawei te volgen en als extra platform te ondersteunen indien er voldoende marktaandeel bereikt wordt.

5.1 Native & Cross platform

Native apps zijn apps gemaakt voor een specifiek platform, Android of iOS. De apps zijn op het device geïnstalleerd vanuit de appstore van de leverancier. Native apps sluiten wat betreft gebruikerservaring aan op het onderliggende platform, ze bieden een goede beveiliging en ze kunnen optimaal gebruik maken van een aantal devicespecifieke mogelijkheden, waaronder de sensoren van het mobiele device, widgets, slimme assistenen en de camera. Native apps worden ontwikkeld met daarvoor bedoelde platformtools. Zowel voor iOS als voor Android is een trend naar declaratief programeren gaande. Voor iOS met Swift UI en voor Android met Jetpack Compose. Hierbij worden user interfaces in code gedeclareerd en wordt gebruik gemaakt van verschillende patterns om user interface en logica te scheiden. Een ander aspect van de native ontwikkeling is mogelijkheid om apps ook op andere platformen van de leverancier te laten draaien. Denk aan infotainment systemen in de auto of zoals bij Apple iOS apps kunnen runnen op MacOS. Native apps bieden dus meeste vrijheid, minste afhankelijkheden en de beste gebruikerservaring maar dienen wel voor elke platform apart te worden ontwikkeld.

- Native, web of hybride? Kies de type app op basis van de eigenschappen van een technologie en maak deze afweging voor elke app opnieuw.
- Android, iOS of Windows? Kies de platformen op basis van de dekkingsgraad bij de doelgroep.
- Gebruik platform richtlijnen en componenten van de platform leveranciers voor het ontwikkelen van native apps.

Cross platform apps zijn ook native apps maar dan gemaakt met ontwikkeltools waarmee voor meerdere platformen apps gemaakt kunnen worden. Voorbeelden hiervan zijn Xamarin, Flutter en React Native. Het grote voordeel van cross platform is een set broncode in één taal voor meerdere platformen waardoor minder specialisatie nodig hebt en potentieel sneller kan ontwikkelen voor meerdere platformen. Het nadeel is natuurlijk dat je vaak net minder flexibel bent en afhankelijk bent van de leverancier. Ook zijn crossplatform apps vaak groter en iets trager dan platform specifieke native apps. Er zijn verschillende manieren waarop cross plaform ontwikkeltools hun apps opbouwen. Voor de user interface kan gebruik gemaakt worden van de native controls of van een eigen controls.

Bij gebruik van eigen controls kan het zijn dat de gebruikerservaring iets afwijkt van de standaard platform ervaring. Voor integratie met sensoren en system SDK's zijn er ook twee mogelijkheden. Wrapping, een dun laagje om de systeem SDK aan te kunnen roepen of plug-ins waarbij per platform een stukje code gemaakt dient te worden, vaak in de taal van het platform. Cross platform apps bieden dus een betere productiviteit en vragen minder diversiteit aan kennis maar vragen altijd om een klein compromis (gebruikerservaring, performance, omvang app) en introduceren extra afhankelijkheden.

5.2 Web & Hybride

Hybride apps is een combinatie van een web app en een native app. De app is gebouwd in HTML5, CSS en Javascript maar draait niet op een server, maar in een container op het mobile device waarbij de code wordt uitgevoerd in een webview, een versimpelde versie van de browser. De webcontent kan in de app zelf zijn opgenomen of worden gedownload via een internetverbinding. Voordeel hiervan is dat de code hergebruikt kan worden voor alle platformen. Voor toegang tot sommige sensoren moet er per platform code geschreven worden, de toegang tot camera, locatie, microfoon is meestal cross-platform beschikbaar. De gebruikerservaring van hybride apps ten opzichte van de gebruikerservaring van native apps is anders. Bijvoorbeeld bij paginaovergangen die door het webgedeelte worden afgehandeld en daardoor minder vloeiend ogen. Hybride apps bestaan in diverse gradaties van "nativeness", dit is verder uitgewerkt in de technische referentie architecturen voor app ontwikkeling. In het hoofdstuk 'Beleid' is aangegeven waar deze architecturen beschikbaar zijn.

Web apps (ook wel HTML5 apps genoemd) zijn apps gemaakt met HTML5- en Javascript-technologie die op een server staan en in de browser van het device uitgevoerd worden. De gebruiker kan door een snelkoppeling op het device te maken toegang tot de app verkrijgen. Bij zogenaamde "installable webapps" wordt een icoon op het homescreen van het device geplaatst. Web apps bieden de ontwikkelaar de meeste flexibiliteit. Voor de ontwikkeling zijn vele ondersteunende frameworks beschikbaar. Interessant zijn met name de Javascript frameworks die allerlei functionaliteiten bieden zoals kant-en-klare componenten. Populaire JavaScript frameworks zijn Angular, React en Vue.

Een bijkomend voordeel van web apps is dat de achterliggende webcode ook ontsloten kan worden in browsers op niet mobiele devices. Door slim gebruik te maken van responsive webdesign heb je op die manier een code base voor alle platformen.

Progressive Web Apps (PWA) is een vorm van web app die steeds populairder wordt. Een PWA wordt bij de eerste request in haar geheel ingeladen. Hierna functioneert de PWA als een opzichzelfstaande applicatie, zelfs zonder internetverbinding. Belangrijkste voordelen van een PWA t.o.v. een web app zijn dan ook gebruikersvriendelijkheid en betere performance.

5.3 Welk type app?

Om de keuze voor een native app, cross platform native, hybride of web app te maken wordt een scorelijst (zoals de tabel hierboven) gemaakt per technologie, met de eigenschappen inclusief een eventuele weging. In de praktijk geven vaak één of twee eigenschappen de doorslag om voor een technologie te kiezen. Maak de afweging voor elke app opnieuw, gezien de snelheid van ontwikkeling van de technologieën en de leercurve van de eigen organisatie.

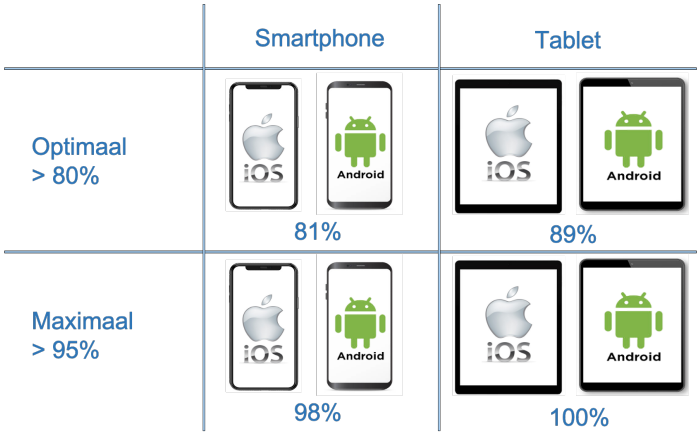
NB: de hier getoonde kruisjestabel is een opvatting en is gebaseerd op de ervaring van de opstellers van dit document en is getoetst aan marktervaring. De tabel pretendeert niet op ieder moment in de toekomst toepasbaar te zijn.

Afwegingen voor app technologie (+ = positief)	Native app	Cross platform native	Hybride app	Web app
Toekomstvastheid	++	+	=	+
Communicatie met backend	+	+	+	++
Update snelheid	=	=	=	++
Ontwikkelkosten	-	=	-	+
Beheer/onderhoud	=	-	-	+
Time to market (1e versie)	+	+	=	++
User experience	++	+	=	-
Animaties en transities	++	+	=	=
Kwaliteit ontwikkeltools	+	+	=	+
Leercurve ontwikkelaar	-	-	-	=
Beschikbaarheid markt ontw. NL	-	=	-	+
Sensoren	++	+	+	=
Native API toegang	++	+	+	--
Beveiliging	++	++	+	+
Toegankelijkheid	+	+	-	=
Offline gebruik	++	++	+	+
Performance	++	+	=	-
Beschikbaarheid app stores	++	++	++	--
Vindbaarheid	=	=	=	+
Push-notificaties	++	++	+	=
Toepasbaarheid Augmented reality	+	=	=	-
Toepasbaarheid Virtual Reality	=	-	-	-
Toepasbaarheid Artificial Intelligence	++	+	=	+

5.4 Mobiele Operating Systems

Apps voor burgers en bedrijven, ook wel **publieke apps** genoemd, kennen een diversiteit aan mogelijke platformen zoals Android en iOS. In de smartphone context is de rol van Windows inmiddels uitgespeeld. Er zijn andere operating systems, maar dit zijn de meest dominante. De huidige wereldwijde (2021) marktaandelen voor de platformen voor smartphones zijn wereldwijd: Android 85% en iOS 15%, de rest is op dit moment niet relevant meer. (bron IDC[14]). De cijfers voor Nederland lijken zowel voor smartphones als voor tablets een iets dominantere positie voor iOS weer te geven, maar zijn moeilijk eenduidig te krijgen. Downloads van een Nederlandse overheidsapp met meer dan 2 miljoen gebruikers laten zien dat hier ongeveer evenveel iOS en IPadOS devices als Android devices mee gemoeid zijn. Bijvoorbeeld DigiD app: iOS 5,7M downloads en Android 5,6M downloads (juli 2021).

Hoe meer platformen ondersteund moeten worden, des te hoger de kosten van ontwikkeling, testen en beheer. Maak daarom een afweging welke platformen ondersteund moeten worden en realiseer je dat niet alle burgers en bedrijven bereikt kunnen worden met mobiele devices. In 2020 gebruikte 84% van de Nederlanders van 12 jaar en ouder een smartphone voor internet toegang, 50% van diezelfde groep gebruikte een tablet. Bepaal voor apps wat het optimaal bereik moet zijn, bijgaande afbeelding geeft hiervan een voorbeeld. 'Optimaal' betekent dat een groot deel van de gebruikers bereikt wordt tegen redelijke kosten. 'Maximaal' geeft aan de eventueel extra te ondersteunen platform(en) zodat bijna iedereen de app kan gebruiken. Dit betekent wel extra kosten.

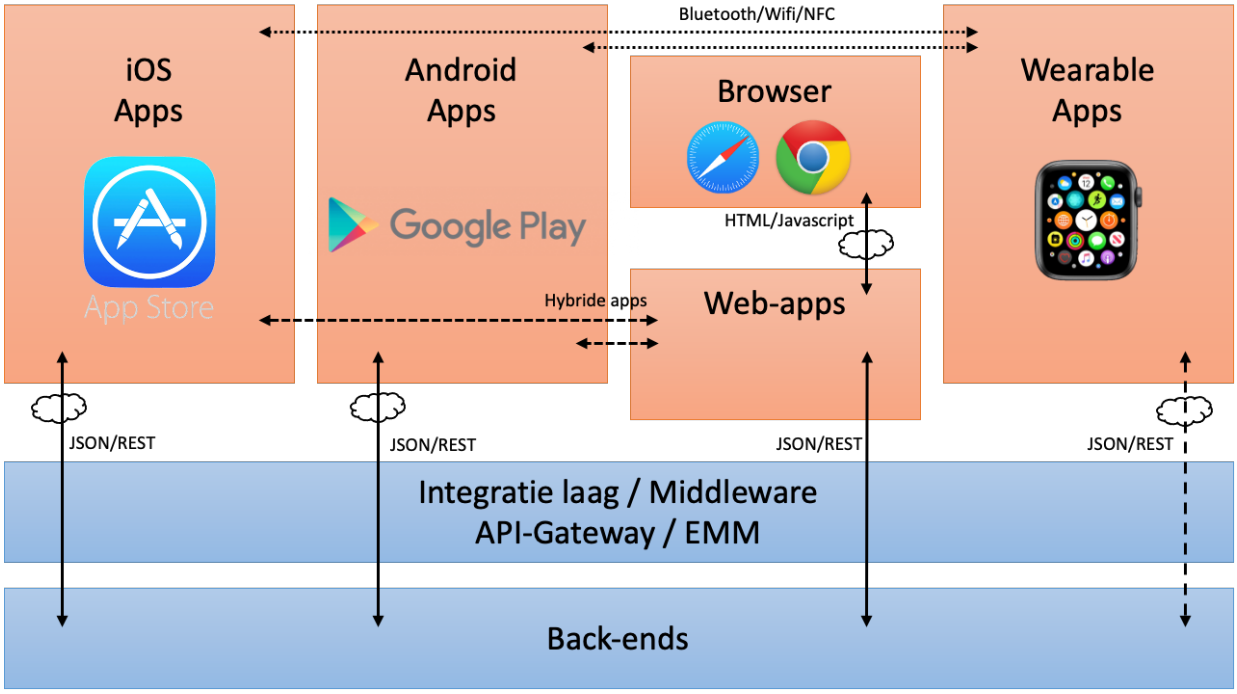


Welke platformen ondersteund worden voor apps voor interne medewerkers, ook wel **enterprise apps** genoemd, wordt niet door de markt bepaald, maar door de organisatie zelf. Default worden meestal iOS en Android ondersteund. De percentages van de platformen zijn op te vragen via de volgende hyperlinks: iOS[15] en Android[16]

[14] https://www.idc.com/prodserv/smartphone-os-market-share.jsp
15 https://developer.apple.com/support/app-store/
16 http://developer.android.com/about/dashboards/index.html

5.5 Componenten van een app

Een app is de front-end van een mobiele oplossing. Een volledige mobiele oplossing bestaat uit meerdere componenten een app, integratie en back-end's. In dit document zijn de backend-componenten niet weergegeven wel zijn de integratiemogeljkheden met back-end uitgewerkt in een apart hoofdstuk integratie. Apps communiceren bij voorkeur met JSON/REST met back-ends om informatie uit te wisselen.



De softwarearchitectuur verschilt per type app:

- **iOS en Android apps.** Beschrijvingen van de softwarearchitectuur voor native apps zijn per operating system zijn te vinden via documentatie-sites van de diverse operating systems zoals iOS van Apple[17] en Developers voor Android[18]. Ook is het mogelijk om te kiezen voor cross-platform technieken als Xamarin, Flutter of Reactive native om iOS en Android apps te maken. Daarnaast kan gekozen worden voor hybride apps, een combinatie van native en HTML5 welke in de app gebundeld is of van de server afkomstig is. Ontwikkeltools als Apache Cordova ondersteunen hierin. Ongeacht de technologie installeert de gebruiker een app op het toestel en de app interacteert middels JSON/REST met back-ends.
- **Web apps.** De ingezette technologie is vooral HTML5, Javascript frameworks en CSS3. Flexibele grids en media queries zijn technieken die hierin gebruikt worden. "Media queries" is een CSS3 module die het mogelijk maakt om content rendering aan te passen aan condities zoals scherm-resolutie (bijvoorbeeld een smartphone versus een high

17 https://developer.apple.com/
18 https://developer.android.com/index.html

definition-scherm). Er zijn ook vele Javascript-frameworks om hierin verder te ondersteunen. De gebruiker start een webapp met de browser of een shortcut op het startscherm. Vaak zal de logica op de server draaien. De webserver van de web-app zal vaak via JSON/REST communiceren met back-ends.

- **Wearable Apps.** Dit zijn apps die op de wearable geinstalleerd worden. Vaak gaat die via een app van de leverancier. Sommige wearables ondersteunen internet verbindingen vanaf de wearable. Andere kunnen alleen communiceren via bluetooth. Wearable apps worden standaard native ontwikkeld met de ontwikkeltools voor het platform: WatchOS, Tizen, Garmin, etc.

5.6 Push-notificaties

Een push-notificatie is een melding die wordt getoond op een device, meestal vanuit een app. Push-notificaties worden gebruikt om iets te melden aan een gebruiker, ook wanneer de app niet actief is. Deze melding kan de vorm hebben van een tekstbericht, een pictogram in de notificatie ruimte op het scherm (Android) of een markering (badge) bij het app-icoon. Push-notificaties hebben relatief geringe kosten voor de verzender doordat er alleen dataverkeer in rekening wordt gebracht, in tegenstelling tot bij SMS-berichten.

- Gebruik push-notificaties niet meer dan strikt noodzakelijk.
- Verwerk geen privacygevoelige informatie in een push-notificatie bericht.
- Maak optimaal gebruik van de beschikbare platform mogelijkheden.

Belangrijke aandachtspunten bij het gebruik van push-notificaties zijn:

- Push-notificaties zijn app specifiek. Alleen als de ontvanger de betreffende app heeft geïnstalleerd, kunnen de berichten worden ontvangen. De inhoud van een bericht moet altijd gerelateerd zijn aan de functionaliteit van de app.
- Ga voorzichtig om met het versturen van push-notificaties, omdat een overvloed aan berichten vaak als hinderlijk wordt ervaren en ertoe kan leiden dat de gebruiker de app weer verwijdert of de push-notificatiefunctie uitschakelt.
- Push-notificaties lopen voor het grootste gedeelte over publieke infrastructuur van de aanbieders van de platformen (Apple, Google). Hoewel deze verkeersstroom encrypted is, impliceert dit dat er een afweging gemaakt moet worden of, en zo ja welke privacygevoelige informatie er in een dergelijke notificatie verstuurd kan worden.
- Gebruik bij voorkeur direct de push notificatie services van Apple (APNS voor iOS) en Google (Firebase voor Android). Indien er gebruik gemaakt wordt van een dienstverlener die dit faciliteert is het belangrijk te checken dat deze dienstverlener geen gebruikersgegevens verzameld en daarmee de privacy van de gebruiker aantast.

- Push-notificaties kunnen zichtbaar zijn op het toegangsscherm van een device (zonder dat er toegang tot het apparaat is gekregen via bijvoorbeeld een pincode). Dit kan afgeschermd worden door een gebruikersinstelling. Echter bij de inhoud van te versturen berichten is deze ongeautoriseerde zichtbaarheid een gegeven om rekening mee te houden.
- Maak ook gebruik van de mogelijkheden die push notificaties bieden: gebruikersacties in de notificatie, geluid, naar de juiste context springen, etc.
- Er is geen directe verbinding met het device van de gebruiker waardoor de afleversnelheid van een bericht niet is gegarandeerd.
- Vraag bij in het in gebruik nemen van een app altijd toestemming voor het mogen versturen van notificaties waarbij een goede onderbouwing voor dit gebruik wordt gegeven. Stel de gebruiker in staat deze beslissing op eenvoudige wijze te herzien. Alhoewel de daadwerkelijke toestemmingsverlening ook een onderdeel is van het onderliggende operating system, is het raadzaam vanuit de app een goede onderbouwing voor het gebruik van de pushberichten te geven om een gebruiker hier een verantwoorde keuze te laten maken.
- Geef een gebruiker - waar mogelijk - invloed op de frequentie en detaillering van de push-notificaties via een instelling in de app, zodat de gebruiker in controle is over o.a. de eigen privacy.

Voor de werking en details van de verschillende push-services wordt verwezen naar de ontwikkelaarspagina's van de verschillende aanbieders: Apple[19] en Android[20]

5.7 Geografische functionaliteit

Mobiele devices bieden, door hun sensoren, geografisch (of locatie) gebaseerde functionaliteit waar apps gebruik van kunnen maken.

Locatie-gebaseerde functionaliteit is in te delen in de volgende categorieën:

- **(Kaart-)visualisatie;** een kaart in een app met relevante ruimtelijke objecten zoals 'points of interest', percelen, gebouwen, wegen en waterlopen. Het kan een tweedimensionale kaart zijn of een 3D 'scene view', een vorm hiervan is een Augmented Reality view van de omgeving.
- **Ruimtelijke analyse;** analyse van ruimtelijke informatie tot afgeleide informatie. Voorbeelden

- Betrek geografische expertise indien nodig.
- Sluit aan op de gangbare Geostandaarden.
- Gebruik overheidsbrede bouwstenen van PDOK.

19 https://developer.apple.com/app-store/review/guidelines/#push-notifications
20 http://developer.android.com/design/patterns/notifications.html

van ruimtelijke analyse zijn reisafstand op basis van huidige locatie en afgeleide omgevingswaarden zoals milieuwaarden per locatie (fijnstof, stikstof) of de kans op bepaalde gebeurtenissen (aardbeving, overstroming).

- **Inwinnen en vastleggen van ruimtelijke gegevens;** registratie van ruimtelijke objecten zoals locaties van objecten (leidingen in de grond, percelen, gebouwen) en registratie van inspecties zoals “de losse stoeptegel” of te vernieuwen wegdelen, of geplande ruimtelijke zaken zoals locaties van braderiekramen. Hierbij kan ook locatiegebonden beeldinformatie worden ingewonnen (foto’s of video’s).
- **Location tracking;** het tracken van de locatie van een device om functies te realiseren als:
    - **Navigatie;** het uitvoeren van een netwerkanalyse voor optimale/gewenste routering van transport.
    - **Geofencing**; een melding bij het naderen of bereiken van een bepaald gebied of bepaalde afstand van een ruimtelijk object of persoon. Beacons (Wikipedia[21]) kunnen een ondersteunende rol spelen bij geofencing.

Het gebruik van geografisch gebaseerde functies is nauw verweven met het domein van Geografische Informatiesystemen (GIS). Dit is een specifiek kennisgebied binnen de ICT waarbij verschillende aspecten meespelen zoals specifieke standaarden, verschillende soorten geodata, overheidsbrede bouwblokken, coördinatenstelsels, kaartprojecties en nauwkeurigheid. Voor meer informatie zie de NORA-pagina over Geo[22].

In het GIS-domein zijn diverse leveranciers[23] actief. Daarnaast zijn er verschillende volwassen Open Source producten zoals web mapping libraries (OpenLayers, Leaflet), GIS-servers (Geoserver, Deegree) en tools voor bewerking en analyse (QGIS, MapWindow). De Publieke Dienstverlening Op de Kaart (PDOK)[24] is een overheidsbrede voorziening waarin allerhande geografische informatie beschikbaar is:

- Basiskaarten/achtergrondkaarten.
- Gegevens uit diverse Basisregistraties: adressen en gebouwen, topografie, kadaster.
- Hoge resolutie luchtfoto’s.
- Allerlei open data sets, zoals natuurgebieden, bestemmingsplannen, etc.

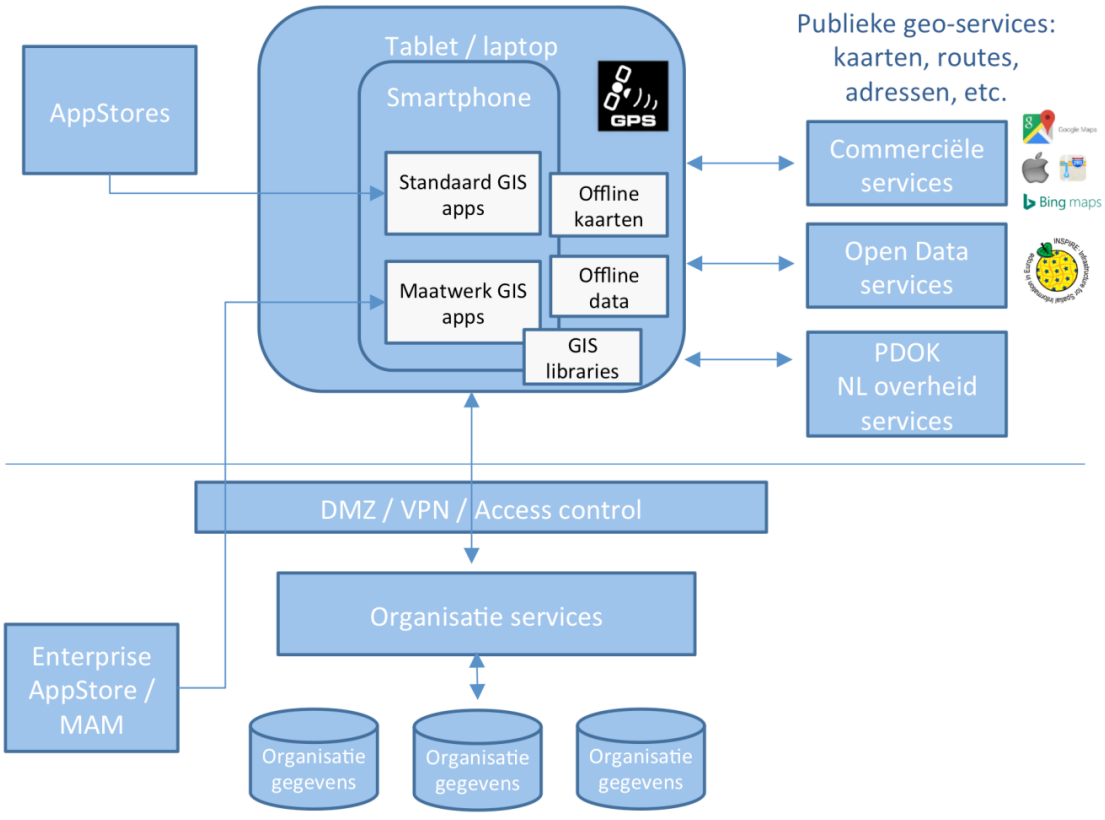
De toegang is hetzij openbaar, hetzij beveiligd via de PDOK toegangslaag.

Verder is er binnen diverse overheden vaak een voorziening ingericht voor toegang tot de diverse Basisregistraties. Daarmee kunnen gegevens zoals kadastrale percelen, NHR-bedrijfsgegevens en adressen en gebouwen worden gebruikt in GIS-enabled apps op mobiele devices. Deze gegevenssets zijn nog rijker dan die van PDOK en kunnen in onderlinge samenhang worden bevraagd.

21 https://en.wikipedia.org/wiki/Bluetooth_low_energy_beacon
22 http://www.noraonline.nl/wiki/Geo
23 https://en.wikipedia.org/wiki/List_of_geographic_information_systems_software#Companies_with_high_market_share
24 https://www.pdok.nl/

Voor ieder van bovengenoemde functies (kaartvisualisatie, ruimtelijke analyse, inwinnen gegevens, location/device tracking) kunnen tools worden ingezet. Het voert te ver om hier alle tools uitgebreid te beschrijven. In de volgende figuur wordt de algemene architectuur van apps met geografische functies weergegeven:

- Er zijn standaard apps beschikbaar in de app stores die gebruik kunnen maken van geografisch gebaseerde functies. Voorbeelden: Google/Apple Maps, en andere, specifiekere mapping apps. Houd de privacy hierbij in de gaten, het feit dat de locatie van iemand door de toepassing kan worden vastgelegd.
- Er kunnen maatwerk-apps ontwikkeld worden binnen een organisatie, die gebruik kunnen maken van de native OS geo functies, maar ook van geo-libraries.
- Apps kunnen offline kaarten opslaan op het device van een beperkt (werk)gebied.
- Apps kunnen geo-gegevens lokaal opslaan en synchroniseren met backendservices.
- Apps kunnen gebruik maken van diverse publieke services: commerciële kaart-functies, open data services, en services van PDOK.nl.



Locatie en Geofencing. Geofencing is het virtueel afbakenen van een geografisch gebied door middel van GPS. De meeste toepassingen vind je terug op mobiele apparaten als tablets en smartphones. Geofencing wordt daarop mogelijk door gebruik te maken van de locatiediensten die tegenwoordig op

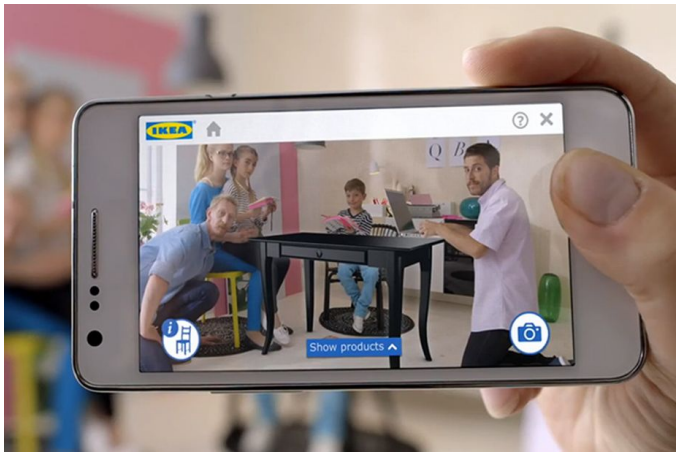
ieder mobiel device geïntegreerd worden[25]. In het algemeen zal geofencing de volgende stappen vergen:

- Bepalen van geofence(s) oftwel 'interessegebieden': geofences ophalen van een service, en/of bepalen op basis van huidige locatie.
- Afhandelen van geofencing events: als het device een geofence binnenkomt of verlaat, of meer of minder dan een bepaalde tijd in een geofence verblijft. Op dat moment kan de gebruiker een notificatie krijgen, en/of er kan een remote service aangeroepen worden om het geofencing event te melden.

Geofencing kan ook bereikt worden door geofences in een backend systeem te registreren en devices periodiek hun locatie te laten sturen naar de backend die vervolgens de geofencing events afhandelt. Dit vereist wel connectiviteit tussen devices en backend. Let bij vastleggen en volgen van locatie en bij geofencing goed op privacy-aspecten.

5.8 Augmented Reality

Bij Augmented Reality (AR) in de mobiele context wordt - evenals bij Virtual Reality - onderscheid gemaakt tussen augmented reality op headsets en augmented reality op apparaten als smartphones en tablets (mobile AR). Deze handreiking focust nu alleen op mobile AR. De toegevoegde waarde van AR in apps is dat digitale gegevens kunnen worden toegevoegd aan een door de camera getoond beeld.



In de API's van Google en Apple zijn mogelijkheden gekomen om AR functionaliteit aan apps toe te voegen. Inmiddels zijn er in de appstores de nodige AR apps beschikbaar. Apple maakt vanaf iOS11 via de ARKit library[26] (een framework voor app-ontwikkelaars) vele nieuwe toepassingen mogelijk op het gebied van AR, die gemakkelijk te integreren zijn in iOS apps. Android realiseert dit via het ARCore[27] framework.

Een aantal toestellen maken gebruik van TrueDepth of Lidar technologie om dieptes nog beter te kunnen inschatten. Test dus altijd in hoeverre de AR app goed werkt voor de verschillende versies van het betreffende operating system en verschillende toestellen.

25 Bron: http://computerworld.nl/security/78231-wat-is-geofencing
26 https://developer.apple.com/arkit/
27 https://developers.google.com/ar/

5.9 Virtual Reality (VR)

Virtual Reality is een kunstmatige, volledig computer-gegenereerde simulatie omgeving of situatie. Hiervoor zijn doorgaans head-mounted displays nodig (HMD's). Hierbij word je volledig ondergedompeld in een virtuele 3D wereld (immersive experience). Er zijn flink wat ontwikkelingen in de VR wereld gaande. Denk hierbij aan 360 graden video (Youtube Facebook 360, Hollywoord VR, VR gaming, Live sports, Social VR, VR chat en VR in de verkoopwereld van auto's en huizen, etc).
Onderscheid moet worden gemaakt tussen VR headsets die zelfstandig werken (zonder smartphone er in gestoken) zoals de Oculus Rift, de HTC Vive en de Sony Playstation VR en mobiele VR headsets waar de smartphone ingestoken wordt, zoals de Samsung Gear VR, de Google Daydream View en de Merge VR Goggles. Deze handreiking beperkt zich tot de mobiele VR headset applicaties.
Complexe VR toepassing kunnen door programmeurs geschreven worden in de Virtual Reality Modelling Language (VRML) waarin objecten worden gedefinieerd. Alternatief is een ontwikkeltool zoals Unity3D waarin VR applicaties gemaakt kunnen worden, geschreven meestal in C#. De in Unity geschreven code kan geconverteerd worden naar IPA files (iPhones) of APK files (Android) en kunnen verder op de standaard manieren gedeployed worden naar de smartphones.

5.10 Conversational user interface

"Conversation", tekst-gebaseerd of voice-enabled interactive communication, is de opkomende user interface die ondersteund moet gaan worden in apps. Het gaat daarbij om ondersteuning van kleine, relevante taken voor de app gebruiker.

Voice-enabled interactie kan via Virtual Private Assistants (VPA) die al zijn ingebouwd in de diverse mobile operating systems . Denk hier bijvoorbeeld aan de virtual assistants zoals Siri[28], Alexa[29] en Google Assistant[30]. Deze VPA's kunnen apps aansturen of de input doorgeven aan een chatbot in de app.

Ook *tekst-gebaseerde input* gaat via een chatbot die daarmee het centrale component vormt in de architectuur.

Houd er rekening mee dat de makers van een VPA mogelijk te zien krijgen wat er aan de VPA gevraagd wordt.

28 https://developer.apple.com/documentation/sirikit

29 https://developer.amazon.com/alexa

30 https://developers.google.com/assistant/sdk/overview

6. Artificial Intelligence

In onderstaand hoofdstuk wordt Artificial Intelligence in de mobiele context beschreven. Om toe te kunnen spitsen op de mobiele implicaties wordt eerst AI in de bredere context bekeken.

6.1 Artficial intelligence: wat is het en definities

Artificial intelligence speelt een steeds grotere rol in de context van mobiel en uiteraard ook daarbuiten

De eerste taak die we ons dienen te stellen is wat Artificial Intelligence überhaupt is. Er zijn vele definities van Artificial Intelligence in omloop. Er is een Europees document over de definitie van AI. Zie hiervoor het volgene document[31] .

- Wanneer AI wordt ingezet denk dan goed na over aspecten van accuratesse, uitlegbaarheid, auditeerbaarheid, transparantie, fairness, ethiek en aansprakelijkheid.
- Denk na over drempelwaardes voor accuratesse die aanvaardbaar zijn. Het gaat hierbij vooral om real-world accuratesse

De vraag moet eigenlijk gesteld worden wat kunstmatig is en wat intelligentie is. Voorlopig willen we in navolging van de Engelstalige wiki (en dan vertaald) als werkdefinitie maar aanhouden het volgende: "*AI is de intelligentie die gedemonstreerd wordt door machines*".

6.2 Strategie voor Nederland en de overheid

In Nederland is er een bredere scope waarin over AI sturing wordt gegeven en visie wordt ontwikkeld en strategie wordt bepaald.
Dat zijn onder andere:

- Strategisch Actieplan Artificiële Intelligentie (SAPAI)[32]. Op 8 oktober 2019 is het strategisch actieplan voor AI gepresenteerd. Het ministerie van EZK&LNV is coordinator Dit strategische actieplan voor AI beschrijft de koers die Nederland wil inzetten op het gebied van AI, en noemt ook concrete acties om de juiste voorwaarden te scheppen om deze koers te realiseren.

[31] https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[32] https://www.rijksoverheid.nl/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificiele-intelligentie

- De AI Coalitie[33] .De AI-Coalitie n Nederland heeft een strategie ontwikkeld voor Artificial Intelligence. Deze coalitie heeft een position paper[34] uitgebracht over de Nederlandse strategie voor AI. Er is een samenhang met de SAPAI.
- Er is normenkader van de hand van het Ministerie van J&V over richtlijnen met betrekking tot het goed omgaan met AI dat mogelijk richtinggevend gaat worden voor de (Rijks)overheid. Er is er ook één van de rekenkamer. Op dit moment is er nog geen compliancy-verplichting met de normenkaders.
- De WRR (de Wetenschappelijke Raad voor het Regeringsbeleid) heeft een rapport geschreven hoe in Nederland het beste kan worden omgegaan met AI. Het is te vinden op: Opgave AI. De nieuwe systeemtechnologie | Rapport | WRR[35].

6.3 Wetgeving, ethiek, richtlijnen en principes

De inzet van AI opereert binnen de bestaande kaders van de wetgeving, die op onderdelen misschien nog niet helemaal voorziet in situaties die kunnen ontstaan door de inzet van AI. Binnen Europa lijkt er wetgeving aan te komen op het gebied van AI (ACT)[36]. Het zal nog enige jaren duren voor zich dat gerealiseerd heeft.

Ethiek, richtlijnen bij Artifical Intelligence

Ethiek keert vaak terug in discussies over AI en ML. ML ethiek is een onderdeel van ethiek in de techniek. AI ethiek kent lange termijn onderwerpen en korte termijn onderwerpen. Bij ethische beslissingen aangaande het wel of niet inzetten van AI en op wat voor manier AI in te zetten kan er vanuit verschillende stromingen naar het issue gekeken worden. De vraag is daarbij welke ethische stroming past bij het tacklen van ethische AI issues en in hoeverre een dergelijk perspectief dan het juiste is en werkt. Veel stromingen zijn denkbaar: Utilitarisme, Plicht-ethiek, Deugd-ethiek, Beginsel-ethiek, Pragmatisme, Intentie-ethiek, Zorg-ethiek, Consequentialisme (gevolgen ethiek), etc. etc. etc….. Om te helpen te komen tot een goede ethiek zijn er vele ethische richtlijnen te vinden. Er zijn wereldwijde, Europese, maar nog geen goede Nederlandse richtlijnen voor het toepassen van AI. De vraag is overigens ook of dat laatste nodig is als er goede Europese richtlijnen zijn.

Van belang zijn de Europese richtlijnen voor AI die op 9 april 2019 zijn uitgebracht en gepubliceerd op deze pagina[37]van de Europese Commissie (Onderaan deze pagina staat de PDF met Guidelines).

Vanuit de mobiele context zijn de richtlijnen van Apple en Google ook relevant:

---

33 www.aicoalitie.nl

34 https://www.vno-ncw.nl/sites/default/files/position_paper_algoritmen_die_werken_voor_iedereen.pdf

35 https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie

36 https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

37 https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

- Google heeft zijn eigen principes en guidelines [38]**Fout! De hyperlinkverwijzing is ongeldig.** (Voor meer informatie pair with Google)[39]
- Apple heeft ook zijn eigen principes en guidelines[40]

In Nederland heeft de AI Coalitie als ambitie om in 2021 tot praktische en gedragen ethische kaders en richtlijnen voor AI toepassingen te komen. Dit betreft dus heel Nederland, niet alleen de overheid.

Principes bij Artificial Intelligence

Een aantal principes kunnen geformuleerd worden en komen regelmatig terug in de diverse guideline documenten. Speciaal verwezen wordt naar de principes genoemd in het AIIA impact assesment document[41] en de ethische principes van de European group on ethics in science and new technologies. Zie hiervoor het volgende document[42]. Onderstaande principes zijn daar deels van afgeleid.

Onderstaande principes zijn daar deels van afgeleid.

1. De AI oplossing dient zeer accuraat te zijn.
   (Trainings/validatie/test/real world). Met name validatie-, test- en real-world accuratesse zijn van belang. Opgepast moet worden voor overfitting en underfitting.
2. AI moet menselijke autonomie respecteren en mag geen inbreuk maken op de menselijke waardigheid.
3. Het AI systeem dient veilig te zijn.
4. Het AI systeem dient fair te zijn en bias dient voorkomen te worden.
   Hierbij gaat het om voorkómen van diverse vormen van vooringenomenheid (bias) op het gebied van ras, sekse, leeftijd etc. Zowel in de data als de algoritmen mag geen bias zitten. Er kan bias in de data zitten, in de modellen en bij ontwikkelaars.
5. Het systeem moet technisch uitlegbaarheid zijn voor zo ver mogelijk.
6. Er moet voldoende transparantie zijn over proces, data en algoritmen
7. Er moet duidelijkheid zijn over aansprakelijkheid bij AI systemen
8. De privacy dient gewaarborgd te zijn in AI systemen.

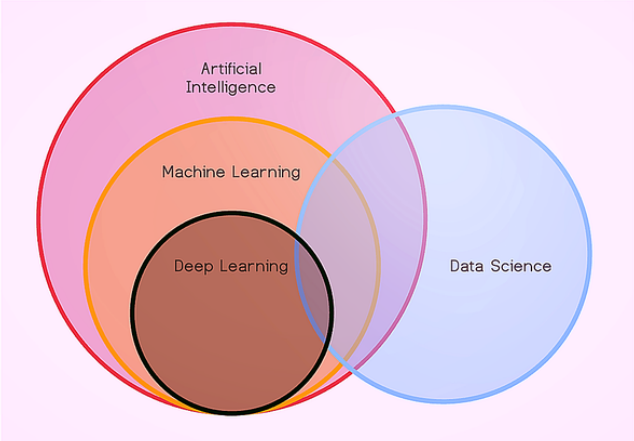
6.4 Machine learning en deep learning

Machine learning zouden we kunnen omschrijven als een specifieke vorm van Artificial Intelligence (AI). *AI is the broader concept of machines being able to carry out tasks in a way that we would consider "smart".*(definitie Forbes)

38 https://ai.google/principles/
39 https://pair.withgoogle.com/
40 https://developer.apple.com/design/human-interface-guidelines/machine-learning/
41 https://ecp.nl/wp-content/uploads/2018/11/Artificial-Intelligence-Impact-Assesment.pdf
42 https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

Machine Learning is a current application of AI based around the idea that we should really just be able to give machines access to data and let them learn for themselves.(Definitie Forbes)

Er ligt een relatie tussen AI, ML, deep learning en data science. Een veelgebruikte weergave van hoe deze zaken zich tot elkaar verhouden of kunnen verhouden is hieronder weergegeven.



bron: Quora (www.quora.com)

Er zijn vele vormen van machine learning. In de mobiele context zal vaak gebruik gemaakt worden van neurale netwerken bij bijvoorbeeld beeldherkenning, spraakherkenning en sentimentherkenning.
Er zijn vele definities van deep learning. Om het te onderscheiden van minder diepe contexten wordt er vaak op gewezen dat er dan sprake is van een meerlaags neuraal netwerk.

6.5 Security en Privacy bij AI

Bij AI kunnen andere soorten aanvallen dan in traditionele software onstaan. Er kunnen aanvallen plaatsvinden die bijvoorbeeld de uitkomst van een beeldherkenning systeem veranderen en daarmee de uitkomst van een beslissing veranderen. Zoals in dit voorbeeld[43].
Wat je zou kunnen doen is bijvoorbeeld veel blijven bijtrainen, zodat de adversarial examples steeds veranderen en potentiële aanvallers ontzettend veel energie moeten stoppen in het voor de gek houden van je applicatie.
Bij het implementeren van gezichtsherkenning of fragmenten van beelden waar personen in voorkomen kunnen weer tot AVG vraagstukken.
Daarnaast speelt ook nog de vraag of een model dat getraind is op persoonsgegevens, zoals beelden

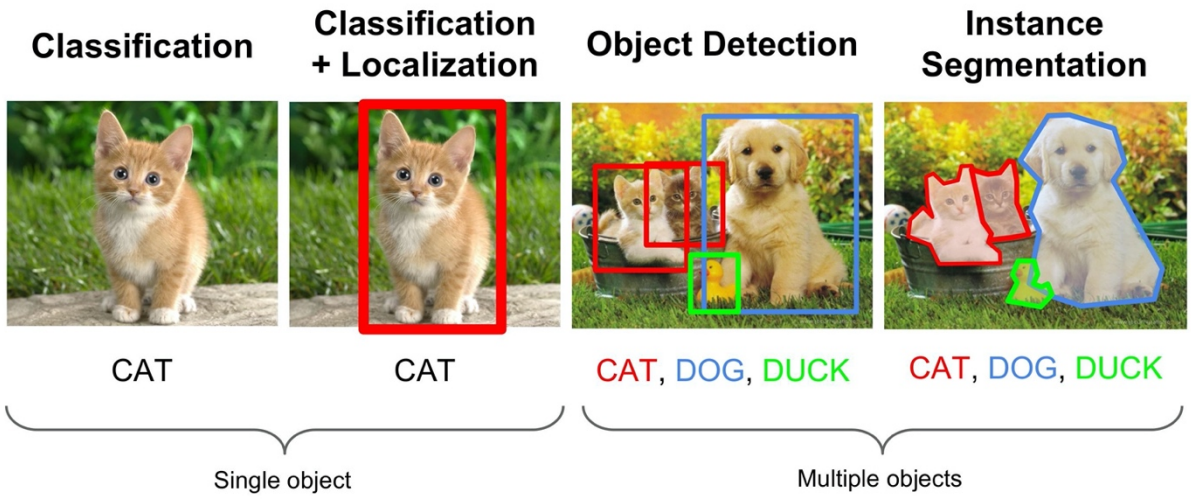
43 https://www.theverge.com/2019/4/23/18512472/fool-ai-surveillance-adversarial-example-yolov2-person-detection

waar personen in voorkomen, ook een persoonsgegeven is, aangezien er door middel van Generative Adverserial Networks soms bepaalde gegevens weer uit het model te halen zijn.
AVG vraagstukken kunnen worden omzeild door synthetische data te gebruiken. Synthetische data is door AI gegeneerde data.
Een ander iets om over na te denken is dat het behoorlijk uitmaakt of algoritmen op een device draaien of in de cloud draaien en aangeroepen worden. Op het gebied van security en privacy heb je dan een andere situatie.
Tenslotte moet er rekening gehouden met het gebruik van externe partijen als onderdeel van het volledige AI gebruik. Er kunnen externe componenten gebruikt worden. Er moet dan goed over worden nagedacht hoe daar mee om te gaan.

6.6 Waar kun je AI voor inzetten?

AI is een breed vakgebied en kent veel interdisciplinaire toepassingen. De twee grootste gebieden waar AI veel waarde toe kan voegen in mobiele context is in de Computer Vision en Natural Language Processing (NLP). Bij beide gaat het om het doen van voorspellingen op complexe data, iets wat lastig is om klassiek te programmeren. Daardoor zijn AI-oplossingen in deze context veel nauwkeuriger, robuuster en kunnen complexere voorspellingen doen dan klassieke oplossingen.

Onder computer vision valt eigenlijk alles dat beeldmateriaal als input heeft. Dit kan zijn een foto, een video of ander beeldmateriaal zoals infrarood- of hittebeelden. Veel gebruikte vormen van computer vision modellen zijn image classification, object detection, en instance segmentation. Een image classification kijkt simpelweg alleen maar naar wat er op de foto staat. Een object detection model kijkt naar wat er op een foto staat en waar dat staat (lokalisatie). Een instance segmentation model kijkt naar de preciese vormen van herkende objecten op een foto. Een ander veel gebruikt model is optical character recognition (OCR). Een OCR-model is een speciale vorm van een object detection model dat kijkt naar welke tekst er op een foto staat.



https://medium.com/zylapp/review-of-deep-learning-algorithms-for-object-detection-c1f3d437b852

Het tweede grote toepassingsgebied van AI is de NLP. Zo wordt AI bijvoorbeeld gebruikt om tekst te begrijpen of analyseren, of om spraak om te zetten naar tekst of andersom. Begin 2020 heeft OpenAI een nieuwe model uitgebracht, genaamd GPT-3, dat tekst kan generen op basis van inputtekst. GPT-3 is bijzonder omdat het generieke taken kan uitvoeren zonder hier specifiek voor getuned te worden. Daarnaast zijn chatbots ook voorbeelden van taalmodellen. Ook kan het vaak heel nuttig zijn om gesproken tekst om te zetten naar geschreven tekst zodat deze dan geanalyseerd kan worden. Zo'n speech recognition model wordt veel gebruikt in virtuele assistenten zoals Siri, Alexa, Cortana, Google Assistant, Bixby, etc. Virtuele assistenten gebruiken dan taalmodellen om te begrijpen wat er gezegd wordt. Daarna praten ze terug door middel van speech synthesis.

6.7 Manifestatievormen van AI op Mobiel

Eigenlijk alle vormen van AI die hierboven besproken zijn kunnen ook toegepast worden op mobiel. Als je AI wilt toepassen op het mobiele platform is het belangrijk om drie vragen te stellen. Die drie vragen worden hieronder besproken.

Bestaat er een standaardoplossing of is het maatwerk?

Voor veel oplossingen die ook maar een beetje generiek zijn is er een standaardoplossing beschikbaar. Voor bijvoorbeeld OCR, spraakherkenning, spraak generatie en verschillende classificatie en detectie vraagstukken bestaan er heel accurate standaardoplossingen. De marktleiders in standaard AI oplossingen zijn Amazon en Google en in mindere mate Apple en Microsoft. Veel van de standaardoplossing draaien in de cloud maar sommige kunnen ook op een mobiel zelf draaien.

Als er een standaardoplossing beschikbaar is het niet logisch om zelf een model in elkaar te gaan zetten omdat je daar veel tijd aan kwijt bent en hoogstwaarschijnlijk geen betere accuratesse kunt behalen.

In het geval dat er geen standaardoplossing beschikbaar is dat kan er gekeken worden naar maatwerkoplossingen. Bij maatwerkoplossingen speelt data een heel belangrijke rol. Als er geen (of niet voldoende) data beschikbaar is kan er geen accuraat model gemaakt worden. Er zijn technieken zoals transfer learning (het pakken van een generiek model en die specifiek maken voor een andere use-case) die kunnen helpen de behoefte naar data te verlagen maar zullen deze nooit wegnemen. Een ML model valt of staat door de kwaliteit en hoeveelheid van beschikbare data.

Wil ik dat mijn AI in de cloud draait of op het toestel zelf?

Het zware werk van voorspellingen doen op basis van complexe data kan op twee verschillende locaties gebeuren, op het toestel zelf of in de cloud. Beide hebben hun voor- en nadelen. Een ML model in de cloud werkt in principe hetzelfde als elke andere endpoint, je stuurt wat op en je krijgt wat terug. Bij een ML model op het device zelf verlaat niets het toestel en wordt de volledige berekening gedaan op de telefoon.

Cloud AI	**Device AI**
Op de cloud is veel meer rekenkracht dus complexere modellen die hogere accuratesses kunnen halen kunnen gebruikt worden.	Op het toestel zelf is minder rekenkracht dus modellen zullen kleiner en compacter moeten zijn om toch snel genoeg te kunnen werken, dit kan ten koste gaan van de acuratesse.
Omdat data naar een server gestuurd moet worden en gewacht moet worden op een reactie zit er een grote latency in. Het analyseren van realtime audio of video is daaroor lastiger.	Doordat er geen data over het internet verstuurd hoeft te worden is er bijna geen latency. Video of spraak kan gemakkelijk in realtime geanalyseerd worden.
Als een model in de cloud draait hoeft er geen rekening gehouden te worden met verschillen tussen iOS en Android.	Doordat het model in de app staat moet op elk platform aparte functies geschreven worden om het model aan te roepen.
Om modellen via de cloud te gebruiken is er een stabiele internet verbinding nodig.	Er is geen internetverbinding nodig om het model te gebruiken als het in de app zelf staat.
Modellen die in de cloud draaien zijn in principe schaalbaar maar kosten voor het hosten van de cloud kunnen een rol gaan spelen.	Modellen die op mobiele toestellen draaien zijn onbeperkt schaalbaar omdat elk toestel de berekeningen voor zichzelf doet.
Doordat het model in de cloud staat is het relatief lastig voor een aanvaller om het model te stelen of kopiëren.	Omdat het model in de app staat is het relatief eenvoudig om het er weer uit te halen. Dat geeft aanvallers de kans om adverserial attacks uit te voeren.
Het model staat in de cloud dus heeft geen invloed op de grootte van de app.	Doordat het model in de app zelf staat zal de app significant groter worden.

Welk ML framework ga ik gebruiken?

De keuze voor het ML framework is afhankelijk van waar het model geplaatst moet worden. Voor deze context zullen drie platformen behandeld worden: iOS app, Android app, Python omgeving (op bijvoorbeeld een server, cloud of een IoT device). Alle frameworks die hieronder beschreven worden hebben de mogelijkheid om hardwareacceleratie in te zetten om nog sneller inference te kunnen doen (dan op een CPU).

Apple heeft voor iOS en MacOS devices zijn eigen ML framework ontwikkeld genaamd CoreML. Qua integratie en functionaliteiten is dit de superieure keuze voor Apple devices. Waar wel op gelet moet worden is dat een model eerst geconverteerd moet worden naar het CoreML formaat. Apple heeft een converter beschikbaar gesteld die o.a. modellen gemaakt met TensorFlow en PyTorch om kan zetten naar het CoreML formaat.

Google heeft in reactie op het CoreML framework hun eigen ML framework gemaakt voor mobiele toestellen genaamd ML-Kit. ML-Kit is beschikbaar voor Android en iOS toestellen en is qua functionaliteit vergelijkbaar met het CoreML framework. Evenals CoreML is ML-Kit een high-level framework wat betekent dat het makkelijk te integreren is in een app, alleen is het minder configureerbaar dan andere frameworks. ML-Kit werkt alleen met modellen die getraind zijn met TensorFlow.

Als laatste bestaat ook nog het TensorFlowLite framework dat een ML Framework is voor edge-devices. Naast Android en iOS draait het TensorFlowLite framework ook op microcontrollers of embedded devices waar Python, Java, Kotlin, Swift, Objective-C of C++ beschikbaar is. TensorFlowLite werkt alleen met modellen die getraind zijn met het TensorFlow framework.

Als laatste is er voor servers of cloud omgevingen ook nog de mogelijkheid om ML-training frameworks te gebruiken voor inference. Zo kan in python omgevingen zoals Django, Flask of FastAPI TensorFlow of Pytorch gebruikt worden om inference te doen. Vaak is dit een makkelijke oplossing voor tests en experimenten, maar in productieomgevingen is het vaak handiger om een framework te gebruiken dat specifiek is voor inference en deployment zoals bijvoorbeeld TensorFlowLite of TensorFlowX.

11 7 Integratiearchitectuur

Een app is vaak onderdeel van een mobiele dienst, waarbij de app communiceert met een achterliggende informatiesysteem (back end), dit valt onder het onderwerp Integratiearchitectuur.

7.1 Standaard producten

Mobiele devices verbinden via het Internet met een backendsysteem in het eigen datacenter of in de Cloud. Om dit veilig en zo beheersbaar mogelijk te maken, is het aan te raden een standaardproduct of combinatie van producten te gebruiken. Het voordeel hiervan is dat de beveiliging gecontroleerd is en up-to-date gehouden wordt door een vertrouwde leverancier. Er zijn twee soorten standaardproducten mogelijk om de communicatie tussen app en backend mogelijk te maken.

- Gebruik standaard producten voor integratie tussen apps en back end systemen.
- Ontwerp diensten en apps voor de toekomst.
- Valideer de schaalbaarheid en beschikbaarheid van back end systemen.
- Gebruik moderne protocollen voor de communicatie.

- **Enterprise Mobility Management (EMM) en zijn opvolger Unified Endpoint Management (UEM)** [44] is een verzameling producten die het beheren van devices en enterprise apps mogelijk maakt. Een onderdeel van het beheren van apps is de mogelijkheid om apps via een Virtual Private Network (VPN) toegang te geven tot het netwerk. Dit kan via de standaard platformmogelijkheden van o.a. iOS en Android. Een aantal producten biedt ook een eigen connectiemogelijkheid vanuit een beveiligde container. Deze laatste biedt voordelen, maar bedenk ook dat er dan een extra afhankelijkheid is om rekening mee te houden bij updates. Platformleveranciers raden het gebruik van containers niet aan omdat zij uitgaan van beveiliging op device-niveau.
- Een **Application Programming Interfaces (API) Gateway** is een product dat diensten door API's beschikbaar stelt voor de buitenwereld. Dit hoeft niet exclusief voor apps te zijn. Met een API Gateway is het mogelijk om de beveiliging en de toegang te regelen en het verkeer te controleren alvorens het door te sturen naar de backend. Een API Gateway kan ingezet worden voor enterprise apps en publieke apps. Enterprise service bus (ESB) producten kunnen hiervoor ook ingezet worden, maar zorg dan wel voor de juiste zonering zoals in de NORA beschreven. In het hoofdstuk 'Infrastructuur- architectuur' wordt dit model toegelicht.

44 EMM\UEM is beschreven in het hoofdstuk 'Beheer en distributie'

7.2 Update strategie

De gebruiker heeft de controle over het updaten van apps. Dit betekent dat in de eerste versie van een app al duidelijk moet zijn hoe met updates omgegaan wordt. Een belangrijke strategie is om de diensten waar een app gebruik van maakt te voorzien van versies. Hierdoor hoeven niet alle gebruikers de app te updaten om gebruik te kunnen blijven maken van een dienst. Als verschillende versies van een dienst niet wenselijk zijn of er moet toch één versie van een dienst uitgezet worden, dan is het belangrijk om dit kenbaar te kunnen maken in de app. Zorg er dus voor dat de app altijd een life cycle management-controle uitvoert. In de praktijk zijn er de volgende mogelijkheden:

- De app is up-to-date, de gebruiker kan de app gewoon gebruiken
- Het advies is om over te gaan op een nieuwe versie, de gebruiker kan de app nog blijven gebruiken
- Er is een verplichting om direct over te gaan op een nieuwe versie, de app is niet meer te gebruiken
- Er is een verplichting om het operating system te updaten vanwege beveiliging, de app is niet meer te gebruiken
- De app is tijdelijk niet bruikbaar vanwege een productie probleem, de app is niet te gebruiken
- De app is end-of-life en wordt niet meer ondersteund

Bij apps voor medewerkers is het wenselijk om een EMM/UEM-oplossing te gebruiken om de nieuwste versie pro-actief te pushen naar de gebruiker en onveilige operating system-versies te weigeren.

7.3 Schaalbaarheid en beschikbaarheid

Apps maken vaak gebruik van de data uit backendsystemen. Deze systemen zullen niet altijd 24/7 beschikbaar zijn voor de app, terwijl gebruikers dat wel verwachten. Indien een backendsysteem niet 24/7 beschikbaar is, zijn er de volgende mogelijkheden:

- Zorg dat de app alleen tijdens de ‘openingsuren’ van het backendsysteem kan werken
- Update het backendsysteem voor 24/7 beschikbaarheid
- Cache informatie in een tussenliggend systeem of in de app zelf zodat de gebruiker niets merkt van het feit dat het backendsysteem niet beschikbaar is. Bij caching in de app heeft deze variant als voordeel dat er ook goed omgegaan kan worden met situaties waar geen verbinding naar het Internet is
- Zorg dat als er offline informatie verwerkt wordt deze op een later tijdstip gesynchroniseerd kan worden

Zorg dat de backendsystemen voldoende schalen om eventuele extra belasting vanuit de app aan te kunnen. Een voorbeeld is de app Telebankieren waarbij het aantal uitvragingen van het banksaldo vele malen hoger is in de app dan via het web. De gebruiker kan namelijk veel sneller (eenvoudig inloggen)

en vaker (altijd mobiel bij de hand) het saldo opvragen. Banken hebben hiervoor hun backendsystemen moeten opschalen.

7.4 Communicatieprotocollen

Communicatie met mobiele devices gaat over een netwerk dat niet altijd snel en betrouwbaar qua beschikbaarheid is. Het is daarom belangrijk om ervoor te zorgen dat de protocol- en formaat-overhead beperkt blijft en dat berichten klein blijven. Het meest gebruikte protocol is JSON/REST en dit wordt goed door alle platformen ondersteund. Naast tekst kunnen ook foto's of video's onderdeel uitmaken van het bericht. Het is raadzaam om in dat geval het bericht op te delen en de relatief grote foto- en videobestanden apart te versturen in een geoptimaliseerd formaat. Uiteraard dient de communicatie altijd over een beveiligde verbinding te lopen, denk aan HTTPS met certificate pinning of een VPN.

7.5 AppConfig

Mobiele operating systemen zoals iOS en Android bieden standaard mogelijkheden voor beheerders om data en apps beter te beveiligen door inzet van een EMM\UEM oplossing. Om apps optimaal configureerbaar te maken, is door een aantal EMM\UEM leveranciers het AppConfig initiatief gestart. Voor verdere informatie zie AppConfig[45] . De meeste van deze voorzieningen vragen geen of een kleine ontwikkelinspanning (bijvoorbeeld het gebruik van een VPN of configuratie parameters). Sommige voorzieningen kunnen zelfs ontwikkelwerk besparen omdat de functionaliteit standaard beschikbaar is, bijvoorbeeld het verbieden van schermafdrukken of copy/paste.

45 https://www.appconfig.org/

12 8 User experience

Hoe voldoen we aan de behoefte van de klant? Hoe kunnen we een app ontwikkelen die eenvoudig in gebruik is en een genot is om mee overweg te gaan? In dit onderdeel geven we handvatten voor een goede gebruikerservaring voor apps. We zullen in dit onderwerp nader ingaan op:

- Belangrijke aandachtsgebieden
- Gebruikers
- Toegankelijkheid (WCAG 2.1)
- Rijksoverheid Huisstijl
- Gebruikersonderzoek

- Een goed ontwerp houdt rekening met meerdere aspecten van de gebruiker en probeert de belasting op de gebruiker zoveel mogelijk te minimaliseren.
- Zorg dat de app voldoet aan de toegankelijkheidseisen eisen van de overheid.
- Maak een afweging tussen Rijkshuisstijl voor en platformstandaarden.

8.1 Ontwerp strategie

Een goed ontwerp is meer dan alleen een mooi kleurvol plaatje met foto's en icoontjes. Een goed ontwerp houdt rekening met meerdere aspecten van de gebruiker en probeert de belasting op de gebruiker zoveel mogelijk te minimaliseren. Er zijn 4 aandachtsgebieden waar je rekening mee wilt houden om tot een goed ontwerp te komen. Deze vier aandachtsgebieden worden uitgelicht in het VIMM ontwerpstrategie:

1. **V**isueel
2. **I**ntelect
3. **M**emory (Geheugen)
4. **M**otoriek

Ontwerp voor visuele impact: Zorg ervoor dat als je aan het ontwerpen ben dat het visueel te begrijpen is. dit kan je doen door de volgende designprincipes te implementeren.

- Zorg ervoor dat de "screenflow" overeenkom met de taskflow
- Zorg voor een goede groepering en labelsysteem
- Maak voorzichtig/bewust gebruik van kleur.

Ontwerp voor Intellect: Zorg ervoor dat het maken van besluiten eenvoudig wordt. Je doet dit door de gebruiker te faciliteren met:

- Previews en eenvoudige manieren om terug te gaan
- Consistent gebruik van componenten
- Goede systeem feedback

Ontwerp voor het geheugen: Een goed ontwerp minimaliseert de geheugenbelasting.

- Maak daarom de opties op het scherm zichtbaar
- Ontwerp voor herkenning en niet voor herinnering
- Het bieden van standaarden

Ontwerp voor motoriek: Minimaliseer beweging afstand en interacties door:

- gebruik te maken van korte afstanden en grote klik oppervlakken
- gebruik te maken van “natural response mapping”
- het reduceren van schermen en stappen

8.2 Gebruiker

Een app wordt ontwikkeld om te voorzien in de behoefte van een gebruiker. Deze behoefte kan voor de hand liggen maar daar mag je als app-ontwikkelteam nooit van uitgaan. Je zal de exacte behoefte zorgvuldig vast moeten stellen en ook hoe je het beste die behoefte kan invullen (app functionaliteit). Bij het vaststellen van de behoefte staat de gebruiker centraal.

Doelgroep vaststellen

Om vast te stellen wie de gebruikers van de app zijn dient een concreet beeld te worden gevormd van de doelgroep. In het hoofdstuk ‘Bedrijfsarchitectuur’ wordt hier al aandacht aan besteed. Hoe concreter het beeld van de doelgroep, des te beter het ontwerp en het eindresultaat. Het ontbreken van een duidelijk beeld van de doelgroep maakt het lastig om een goede app te ontwerpen. Weten wat er leeft bij de doelgroep, welke behoeftes er zijn of welke problemen men ervaart, bepaalt de impact van de app op de uit te voeren taken door de gebruiker.

Er zijn vele manieren om je doelgroep te leren kennen en er een beeld van te vormen. Een doelgroepanalyse en persona's kunnen bijvoorbeeld enorm helpen om vanaf het begin de juiste ontwerpbeslissingen te nemen. Hoe duidelijker het beeld van de gebruiker, des te beter er bepaald kan worden wat de juiste informatiestructuur, interactie, beeldmateriaal en ‘tone of voice’ teksten moeten zijn.

Doelgroepanalyse

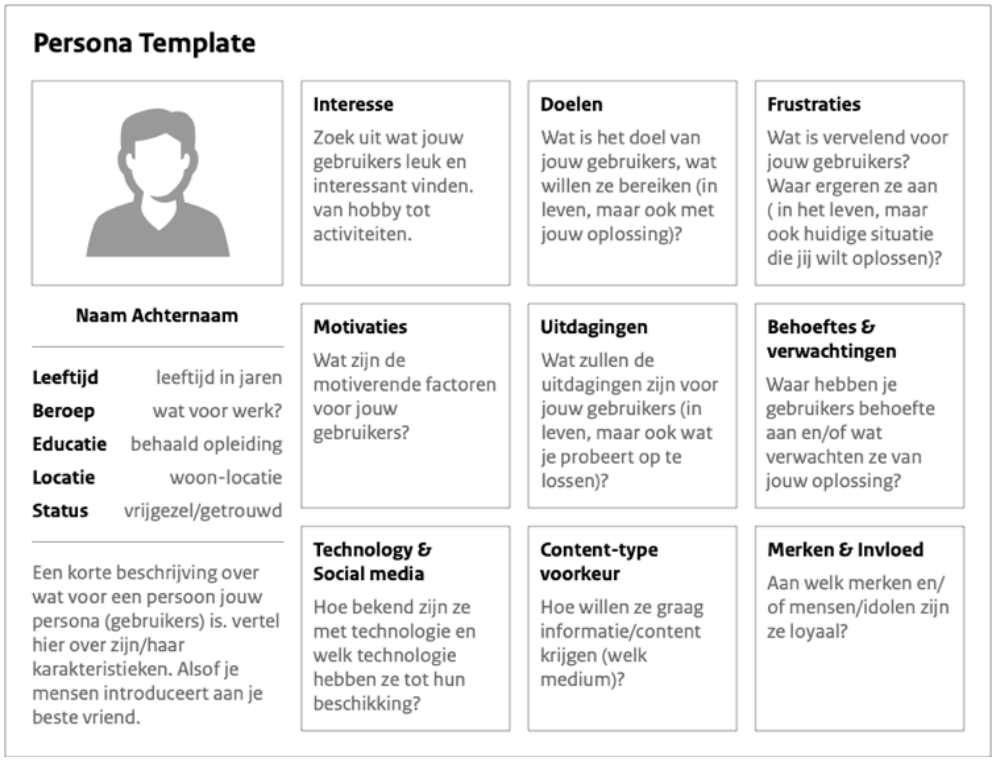
De doelgroepanalyse is breed en geeft antwoord op vragen als:

- Welk type gebruikers helpen we?
- Wat verwachten de gebruikers?
- Onder welke omstandigheden moet de primaire taak worden uitgevoerd?
- Met welk apparaat?
- Zijn er problemen of onduidelijkheden bij het gebruik?
- Welke sites of applicaties gebruiken ze nog meer?

Hiermee kun je een gebruiksgericht concept opstellen of persona's ontwikkelen.

Persona's

Een persona is een nauwkeurige omschrijving van iemand uit de doelgroep Reden om ze te maken is dat een levendige beschrijving van een persona veel beter werkt dan de droge opsomming van een doelgroepomschrijving. Wanneer een product zoals een app sterk focust op de persona, des te beter de gebruikerservaring (‘user experience’).



Gebruikersonderzoek

Het belangrijkste doel van gebruikersonderzoek is om vanuit het perspectief van de gebruiker te kijken. Gebruikersonderzoek vertelt ons:

- Welke personen de app gebruiken
- in welke situatie gebruikers de app gebruiken
- wat ze verder nodig hebben

Enkele voorbeelden van veel gebruikte onderzoeksmethoden:

Interviews: Een-op-een-interviews zijn een goede methode om te gebruiken als je diepgaande / gedetailleerde data wilt verzamelen van een gebruiker. Het helpt om een beeld te krijgen van de gebruikersperspectief en zijn ideeën.

Enquêtes: Een Enquête is een goede methode voor het verzamelen van gegevens met de mogelijkheid om snel informatie te vergaren over een breed publiek. Het verzamelen en analyseren van gegevens kan worden geautomatiseerd om tijd en kosten te besparen.

Usability tests: Usability testen is het proces waarbij potentiële gebruikers de app ervaren in een observeerbare omgeving. Het zijn evaluaties met als doel feedback te ontvangen en weloverwogen ontwerp beslissingen/verbeteringen door te voeren.

Expert review: Bij een expert review evalueren experts de app op basis van hun ervaring en kennis op het gebied van user experience. Tijdens de expert review is de gebruiker het belangrijkste referentiepunt en wordt de analyse gedaan binnen de context van bedrijfsdoelstellingen en de algehele ervaring.

Specifieke en taakgerichte apps

Een app richt zich idealiter op het uitvoeren van één specifieke taak. Maak van een app daarom geen portaal met een waaier aan verschillende functionaliteiten en keuzes zoals een website dat doet. Meerdere verschillende functionaliteiten maken de app meestal te complex, wat doorgaans een negatief effect op de gebruikerservaring kan hebben. Focus dus op de primaire taak van een app, deze dient direct duidelijk te zijn. Hoe duidelijker de taak, des te intuïtiever de app zal aanvoelen in het gebruik.

8.3 Toegankelijkheid

Gebruikers met een beperking moeten de app kunnen gebruiken. Meer specifiek dient er rekening gehouden te worden met:

- waarneming
- begrip
- navigatie
- communicatie
- Input

Toegankelijkheid omvat alle handicaps die van invloed zijn op het gebruik van de app, waaronder:

- gehoor
- verstand
- neurologisch
- fysiek
- spraak
- zicht

Verplichting voor apps van overheid

Sinds 1 juli 2018 is het Tijdelijke besluit digitale toegankelijkheid overheid van toepassing op de apps van Nederlandse overheidsinstanties. Volgens het besluit moeten apps voldoen aan:

- WCAG 2.1 niveau AA. (bouwt voort op (WCAG 2.0)
- verantwoording middels een toegankelijkheidsverklaring.

Vanaf 23 juni 2021 is elke overheidsorganisatie verplicht een toegankelijkheidsverklaring op te stellen voor elk van haar apps.

Standaarden: De eisen voor digitale toegankelijkheid komen voort uit de Web Content Accessibility Guidelines (WCAG) versie 2.1. Voor de overheid geldt dat apps aan de regels op level A en AA moeten voldoen.

Ondersteuning: Er zijn diverse organisaties die kunnen ondersteunen bij het toegankelijk maken en/of testen van apps.

Toegankelijkheid best-practices: Toegankelijkheid (accessibility) is op te delen in vier categorieën waar aandacht aan besteed moet worden om een platform en/of app toegankelijk te maken voor mensen met beperkingen:

Visuele beperkingen

Van kleurenblindheid, slechtziende t/m volledige blindheid. Het is belangrijk dat apps voldoen aan:

- Voldoende contrast tussen voor- en achtergrond content
- Groot lettertype of de mogelijkheid om grootte te kunnen aanpassen
- Mogelijkheid om in te kunnen zoomen
- Correcte hiërarchie in content (denk aan H1, H2, H3, Body, etc) voor screenreaders
- Zorg voor goede ondersteuning van 'Voice over' voor iOS en 'Talk back' voor Android.
- Alt-tekst en Caption voor afbeeldingen en links, bedoeld voor screenreaders
- Gebruik altijd kleur in combinatie van tekst (kleurblindheid)

Gehoorbeperkingen

Hou rekening met gehoorbeperkingen indien je gebruik maakt van audio. Pas captions voor audio, video en andere non-tekstuele content toe. Denk daarbij aan:

- simpele woorden, vertalingen en subtitels
- links en knoppen die duidelijk zijn (waar gaat het over, wat gaat er gebeuren).
- Ontwerp voor standaarden (browsers, screenreaders, speech-to-text software, etc.)

Motorische beperkingen

Hou rekening met Ouderen,mensen met fysieke beperkingen en mensen die bepaalde software en/of hardware moeten gebruiken vanwege hun werk/situatie (denk aan voice-to-command tools, speciale muis/toetsenbord).

- Zorg dat het klik oppervlak van knoppen groot genoeg zijn
- Zorg ervoor dat knoppen/interactieve elementen binnen de duim-bereikbaarheid zijn.
- Ontwerp/ontwikkel voor standaarden (browsers, verschillende devices, etc.)
- Ken je doelgroep

Cognitieve beperkingen

Door content, woorden, jargon en navigatie zo simpel en duidelijk te houden, kunnen mensen met een cognitieve beperking een app beter begrijpen en gebruiken.

- Geef hints en hulpmiddelen (denk aan placeholders, tooltips, etc) zodat een gebruiker altijd weet wat hij moet doen en/of hoe hij verder kan.
- Geef empty-states zodat gebruiker begrijpt hoe hij verder moet om bijvoorbeeld iets te kunnen toevoegen.
- Een eenvoudige onboarding kan gebruiker helpen bij het begrijpen wat een app
- Gebruik iconen in combinatie met tekst, iconen zijn niet altijd vanzelfsprekend.
- Zorg dat mensen zien en begrijpen i.p.v. herinneren, zo min mogelijk geheugen-overload.

8.4 Rijkshuisstijl

Apps voor de Rijksoverheid moeten voldoen aan twee typen standaarden, de huisstijl van de organisatie (voor de Rijksoverheid is dit de Rijkshuisstijl voor apps) en de standaarden die door de leveranciers van de platformen (Apple en Google) worden uitgegeven. Daarnaast zijn er algemene richtlijnen voor het ontwerpen van een app, bijvoorbeeld de standaarden vanuit het W3C, een organisatie die als doel heeft de interoperabiliteit van het World Wide Web te verzekeren.

Het is van belang te voldoen aan de Rijkshuisstijl voor apps, echter wanneer dit botst met eisen op het gebied van toegankelijkheid, dan gaan de eisen voor toegankelijkheid voor.

Wanneer de design guidelines van Apple en Google botsen met de Rijkshuistijl voor apps, dan wordt er meestal voor gekozen om de Design Guidelines van Apple en Google te volgen.

Huisstijl van een organisatie

De rijkshuisstijl voor apps is randvoorwaardelijk voor een herkenbare en toegankelijke Rijksoverheid. Door de invoering van één app huisstijl is de Rijksoverheid direct als afzender herkenbaar. De Rijkshuisstijl bevat standaarden voor o.a.:

- afzenderschap
- launchscreen
- logo’s
- kleurgebruik
- lettertypen
- iconen
- navigatie

Hieronder volgt een samenvatting van deze standaarden, zie voor een uitgebreide beschrijving de online stijlgids met basiselementen.

Afzenderschap

Het afzenderschap in een app wordt weergegeven door middel van het logo: beeldmerk (blauw lint) en woordmerk (organisatienaam). Het lint staat bij apps altijd bovenaan, in het midden en alleen op de launchscreen.

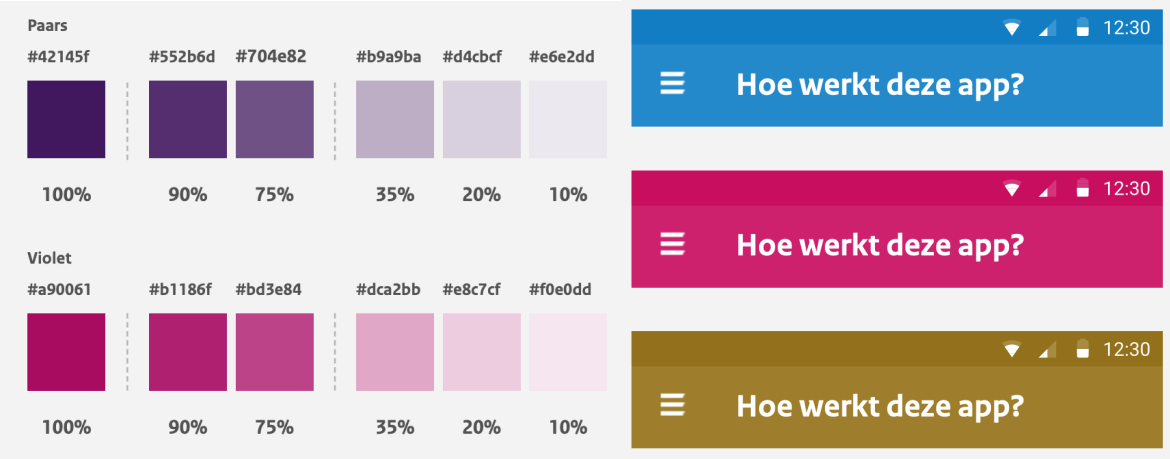
Launchscreen en logo’s

Het Launchscreen is het eerste scherm dat wordt weergegeven. Het doel van dit scherm is om de gebruiker feedback te geven dat de app geladen wordt.

Voorbeelden van launchscreens met logo

Kleurgebruik

Elke organisatie dient een specifieke set van hoofd- en afgeleide kleuren te gebruiken.

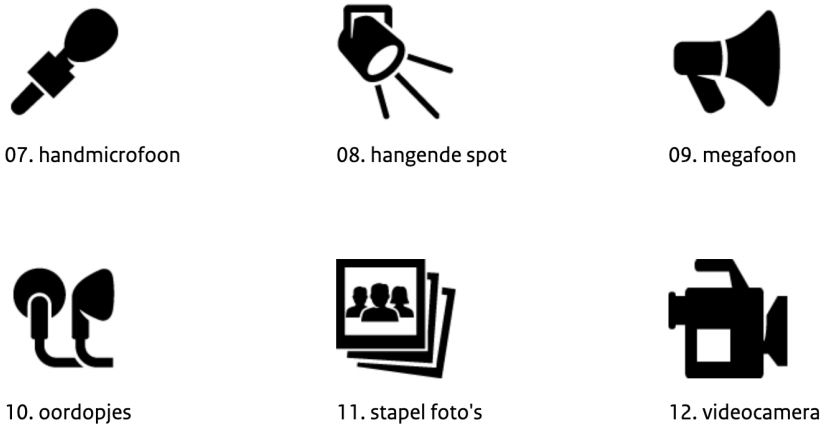


Voorbeelden van kleurensets

De nieuwste versies van iOS en Android bieden aan de gebruiker de mogelijkheid om voor een lichte of donkere instelling te kiezen, zorg voor beide instellingen met een goede kleurenset uit de huisstijl. De huisstijl is vaak van oorsprong opgezet voor traditionele media en wordt steeds meer geschikt gemaakt voor digitale communicatie.

Iconen

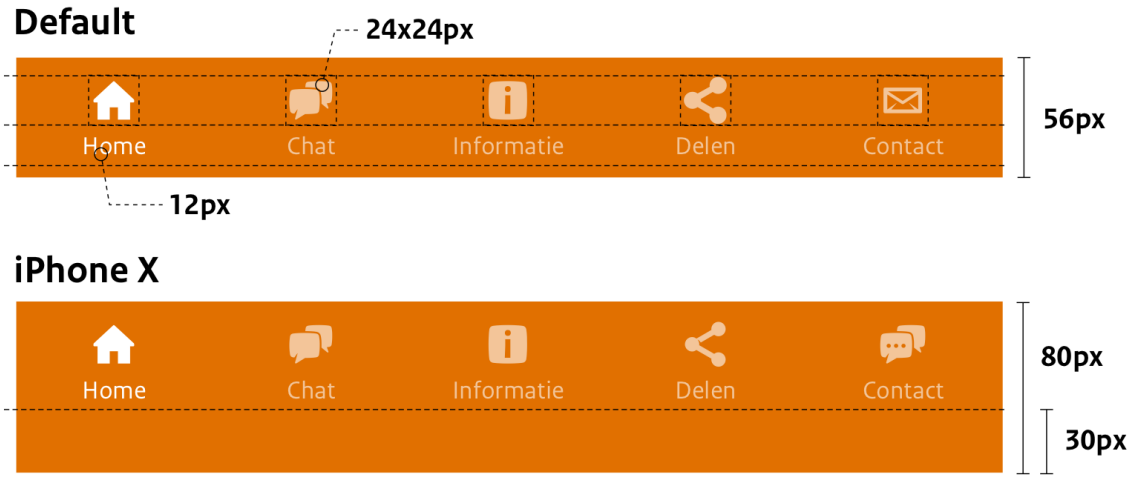
Binnen een app kan gebruik worden gemaakt van iconen waarvoor vanuit de Rijksoverheid richtlijnen zijn opgesteld. Ook is er een iconenbibliotheek beschikbaar.



Voorbeelden uit de iconenbibliotheek

Navigatie

Herkenbare en gebruiksvriendelijke navigatie is van groot belang voor de bruikbaarheid van een app. Daarbij gaat het om menu's, buttons, sliders en selection controls.



Beschrijving van de bottom-navigatie met (maximaal) 5 acties

Organisatie specifieke richtlijnen

In sommige gevallen kan het toepassen van de huisstijl conflicten opleveren met het conformeren aan leveranciers standaarden. Een aantal ontwikkelorganisaties binnen de overheid heeft daarom eigen richtlijnen en iconensets gemaakt zoals de Belastingdienst en Defensie. Geadviseerd wordt de huisstijl zoveel mogelijk toe te passen als binnen de platform specifieke richtlijnen mogelijk is.

Design system

De rijkshuisstijlwebsite met de hierboven genoemde hulpmiddelen kan je zien als een design system: een centrale omgeving waarin alle bouwstenen van digitale diensten en producten van een organisatie staan. Uit deze bron kunnen alle bouwteams putten (webdevelopers, appdevelopers, webredactie maar ook de afdelingen communicatie en marketing). Doordat iedereen dezelfde bouwstenen gebruikt om de diensten en producten op te bouwen, is er een verregaande consistentie in design en (digitale) communicatie. En dus ook in de gebruikerservaring.

Moderne design systems gaan echter verder dan de rijkshuisstijlwebsite, die bieden interactie-patronen, componenten-bibliotheken, templates, ontwikkeltools e.d. voor nog meer kwaliteit en consistentie en het voorkomen van dubbel werk. Diverse overheidsorganisaties hebben een eigen design system of zijn dat aan het opstarten. En er is ook een breder initiatief: het, nog in ontwikkeling zijnde, NL Design System, een initiatief van Gebruiker Centraal en Code for NL in nauwe samenwerking met Common Ground, DUO, Gemeente Den Haag, Mens Centraal en vele andere partijen.

13 Infrastructuur-architectuur

Specifiek voor de infrastructuur en architectuur van apps is zonering, connectiviteit en het grote aantal ICT-componenten die deel uitmaken van een mobiele dienst.

9.1 Infrastructurele zonering

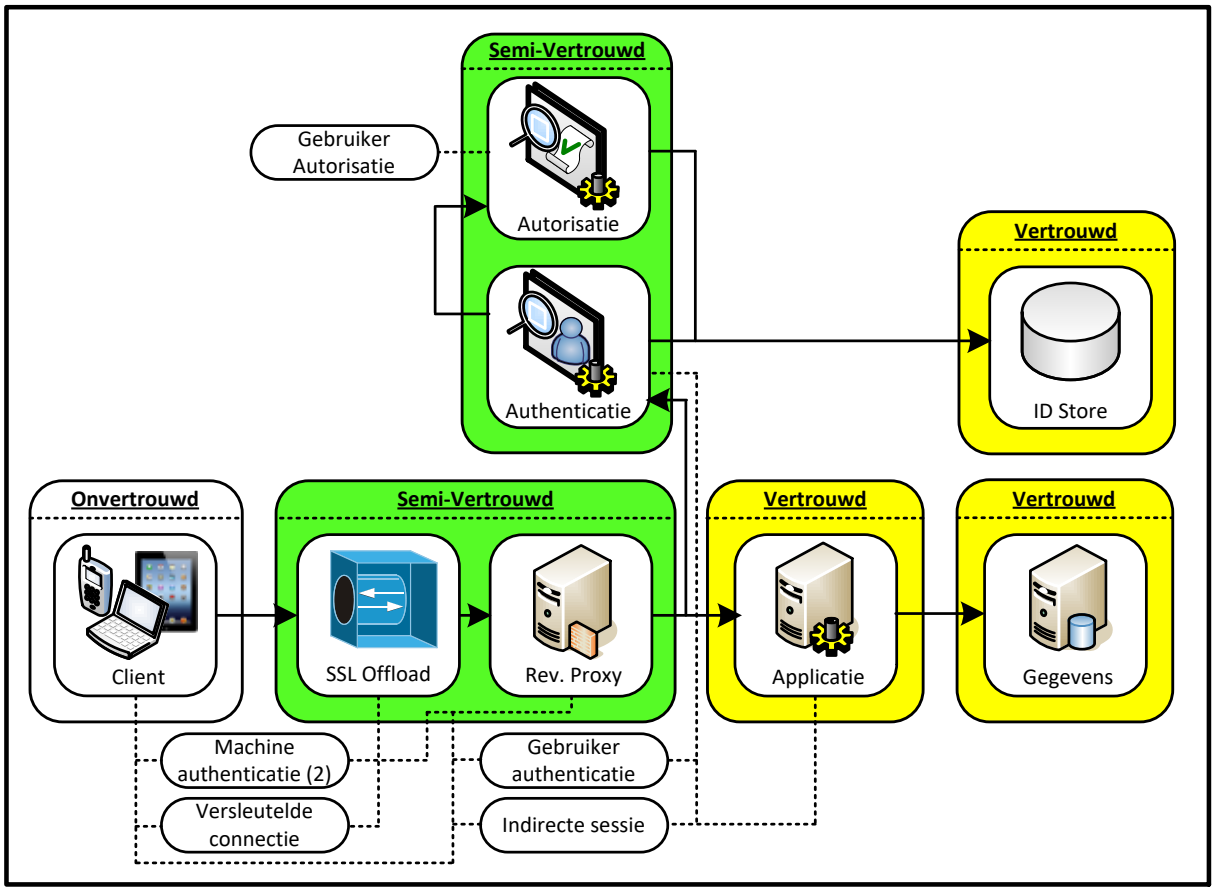
De afbeelding in deze paragraaf is een weergave van de zonering in de infrastructuur voor een app die op een mobiel device draait en verbonden is met een backendsysteem. Dit zoneringsmodel leunt sterk op het NORA beschouwingsmodel voor zonering[46].

Gebruikers moeten systemen uit de interne vertrouwde omgeving vanuit een externe onvertrouwde omgeving (Internet, 3G, 4G) kunnen gebruiken. Volgens het infrastructurele zoneringsmodel moet verkeer vanuit de zone Onvertrouwd naar de zone Vertrouwd mogelijk zijn. Vanwege beveiligingsredenen is het niet toegestaan dat verkeer een zone overslaat, bijvoorbeeld als een informatiesysteem een rubriceringsniveau heeft waarbij het alleen toegestaan is dat de gegevens door vertrouwde devices worden benaderd. In de BIO[47] is opgenomen dat alleen vertrouwde devices gekoppeld mogen worden aan het vertrouwde netwerk. Vaststellen van dit vertrouwen vindt dus altijd plaats buiten deze vertrouwde zone; in een DMZ (semi vertrouwde zone).

- Devices zijn elementen in de ICT -infrastructuur met eigen spelregels.
- Zorg voor een goede OTAP omgeving inclusief representatieve devices om te testen.
- Zorg voor schaalbaarheid voor wat betreft de capaciteit van backend systemen en andere infrastructurele componenten.

46 https://www.noraonline.nl/wiki/Beschouwingsmodel_zonering
47 https://www.noraonline.nl/wiki/BIO_(Baseline_Informatiebeveiliging_overheid)

De volgende afbeelding geeft weer hoe de zonering er uit ziet.



Nb. Bij gebruik van EMM\UEM-tooling kan het er enigszins anders uit zien (ook afhankelijk van de specifieke tooling). Deze afbeelding beschrijft de infrastructuur van een app die draait in een omgeving zonder dergelijke voorzieningen.

9.2 OTAP-omgeving

De ontwikkeling van mobiele oplossingen vereist een ontwikkel-, test- en acceptatieomgeving (OTA) naast de productieomgeving (P). Alle componenten die deel uitmaken van de keten die een mobiele oplossing tot stand brengt, moeten beschikbaar zijn in de OTA, bijvoorbeeld een EMM\UEM-oplossing. Het is essentieel voor de ontwikkeling dat het ontwikkel- en testteam beschikt over een representatieve set van mobiele devices die een afspiegeling vormen van de door de doelgroep gebruikte mix aan devices. Het is, zeker bij apps voor het publieke domein, onmogelijk om alle soorten mobiele devices en operating system-versies “in huis” te hebben. In dergelijke situaties kan het een mogelijkheid zijn om apps op een marktconforme set devices te testen door gebruik te maken van mobiele test-oplossingen in de cloud. Deze oplossingen bieden fysieke devices die door geautomatiseerde testen gebruikt kunnen worden. Let hier wel op of een dergelijke opzet in lijn met het beveiligings- en privacybeleid van de betreffende organisatie is.

Bij de afweging of er een OTAP-straat ingericht wordt voor de EMM/UEM en/of een app, spelen diverse criteria:

- Financiën;
- Beveiligingsaspecten;
- Beheerlasten;
- Heeft de back-end van een App een OTAP straat?

In de praktijk komen er, mede afhankelijk van een volwassenheidsstadium, combinaties voor zoals: OP of OAP. Het komt ook voor dat er een Opleidingsstraat wordt ingericht.

9.3 Schaalbaarheid

Een mobiele dienst bestaat uit een groot aantal ICT-componenten die samen het succes bepalen, zoals:

- Directory-services;
- VPN-diensten;
- Databasesystemen;
- Back-endsystemen (mail, webservices);
- Devices;
- Telecomnetwerken;
- EMM/UEM;
- AppStore(s).

Een mobiele dienst heeft impact op de capaciteit van de infrastructuur. Zorg er voor dat de netwerkinfrastructuur flexibel en schaalbaar is. Bij een mobiele dienst is de verhouding tussen devices en gebruikers essentieel anders dan bij een klassieke werkomgeving. Bij deze laatste is er een vast aantal werkplekken waarop de achterliggende infrastructuur berekend en geschaald kan worden. Bij de mobiele diensten zijn er meerdere devices per gebruiker, met veel variatie in aantallen. Dit is moeilijker voorspelbaar en planbaar. Een goede monitoring en anticiperend vermogen op capaciteit binnen de gehele infrastructuur is een vereiste voor mobiele diensten. Als bijvoorbeeld E-mail op mobiele devices aangeboden wordt, is van te voren belangrijk om na te gaan of het huidige mail systeem hier op geschaald is. De belasting van het mailsysteem kan twee tot drie keer toenemen aangezien gebruikers van één naar twee of drie devices gaan. Houd ook rekening met sterke toename van de netwerkbelasting, zeker als men gebruik gaat maken van VPN-connectiviteit.

Het gebruik van de Custom Store, Managed Store en unlisted Apps kan de belasting van het interne systeem bij installaties verminderen.

.

9.4 Connectiviteit

Bij het gebruik van apps op een mobiel device is connectiviteit essentieel om de gegevensuitwisseling tussen de app en de achterliggende backend systemen te kunnen realiseren. Voor apps is dit essentieel anders dan voor applicaties in een klassieke enterprise-omgeving. Er zijn twee vormen van mobiele connectiviteit:

- WiFi bestaat er in diverse technische varianten met elk hun eigen kenmerken qua bereik en capaciteit. WiFi kan gecontroleerd worden aangeboden in een bedrijfsomgeving. Hierdoor is er invloed op deze beide parameters. Bij WiFi in de openbare ruimte (Hotspots) en huiselijke omgeving is deze invloed er niet. De steeds hoger wordende penetratie van WiFi in de huiselijke omgeving heeft een nadelige invloed op het bereik en de capaciteit van een thuisaansluiting. Immers het signaal houdt niet op bij de buitenmuren en steeds meer netwerken willen gebruik maken van de beperkte frequentieruimte die voor WiFi beschikbaar is.
- De landelijke mobiele netwerken bieden datatransmissie aan op basis van 3G,4G en 5G technologie. Binnen deze netwerken is het slechts beperkt mogelijk bedrijfsmatige beheerde omgevingen af te nemen. Daarnaast is bereik niet gegarandeerd. De meeste providers leveren weliswaar een landelijke dekking, echter gebaseerd op gebruik buitenshuis. Indoor dekking wordt primair bepaald door de constructie van het gebouw.

Belangrijke parameters bij deze twee vormen van connectiviteit zijn bereik en capaciteit. Beide zijn randvoorwaardelijk om een goede user experience te kunnen bieden. Afhankelijk van de functionaliteit en doelgroep van de app dient er ook rekening mee gehouden te worden dat connectiviteit niet gegarandeerd is. Bepaalde apps zullen dus ook zonder een connectie met hun backend, dus offline, moeten kunnen functioneren. Aandachtspunt hierbij is een veilige opslag van data bij databewerking. Bij apps die met latency-gevoelige data werken (bijvoorbeeld beeld en geluid) is een voldoende netwerkcapaciteit een vereiste.

Gebruik van (commerciële) connectiviteit is niet gratis. Houd er, zeker bij publieke apps, rekening mee dat de benodigde transmissiecapaciteit in overeenstemming is met het doel van de app en de gebruikersgroep. Deze gebruikskosten liggen immers bij de gebruiker van de app en niet bij de aanbieder.

Het is belangrijk bij het testtraject ook de stabiliteit van de app te testen onder wisselende bereikbaarheidsscenario’s, zoals een kwalititatief slechte verbinding, lage bandbreedte enz.

9.5 Cloud

Het gebruik van clouddiensten en -technieken neemt toe. De (Rijks)overheid heeft van oorsprong een terughoudend beleid ten aanzien van het gebruik van publieke clouddiensten. Via het inrichten van overheids-datacentra worden de interne ICT-voorzieningen ingericht als een private cloud. Voor de ontwikkeling en beheer van apps kunnen desondanks wel clouddiensten of -technieken worden ingezet, waarbij dan wel een zorgvuldige afweging moet worden gemaakt of hier publieke of private cloud wordt gebruikt, zoals:

- Welke gegevens ga ik verwerken; hoe vertrouwelijk of privacygevoelig zijn deze?
- Waar vindt deze verwerking geografisch plaats?
- Aan welke wet- en regelgeving ben ik als opdrachtgever dan gehouden?
- Welke waarborgen kunnen er met de aanbieder worden overeengekomen? Welke contractuele afspraken zijn er mogelijk?
- Is er een goede exit-strategie mogelijk?

Vanuit het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties is er door DGOO/CIO-Rijk een handreiking dataopslag gemaakt die hier behulpzaam bij kan zijn. Deze is verkrijgbaar via het secretariaat [48]van DGOO

48 secretariaatCIORijk@minbzk.nl

14 Beveiliging

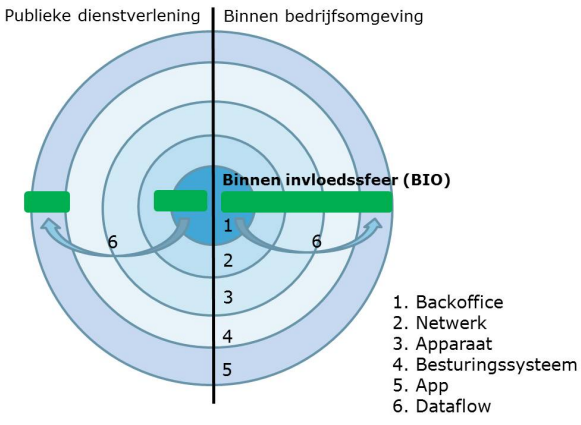
Het aanbieden van diensten via een app, zeker in het publieke domein, brengt diverse uitdagingen met zich mee op het gebied van beveiliging. Het is zaak de gegevens die met de app en gebruiker worden gedeeld goed te beveiligen. Deze beveiliging is vereist, ongeacht de vraagstelling of de overheid de eigenaar of een bewerker van de gegevens is.

10.1 Beveiliging en de overheid

Net als iedereen dient ook de overheid zich aan de wet te houden. Om aan de wetgeving te kunnen voldoen, is vanaf 1 januari 2020 binnen de overheid de Baseline Informatiebeveiliging overheid (BIO)[49] in gebruik. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. De BIO is een verzameling van kaders en richtlijnen waar alle aspecten met betrekking tot ICT-dienstverlening (bedrijfsvoering, processen, personeel en infrastructuur) aan dienen te voldoen.

- Voer per app een risicoanalyse uit en kies de juiste mix aan beveiligingsmaatregelen voor de app.
- Publieke apps dienen intrinsiek veilig te zijn. Voor enterprise apps kan er eventueel gebruik worden gemaakt van EMM/UEM-voorzieningen.
- Bij publieke apps is er een reëel risico op nagemaakte of gemodificeerde varianten (cybercriminaliteit), houd hier rekening mee.

Bij enterprise apps is er een end to end invloed op de beveiligingsmaatregelen, bij apps met gebruikers in het publieke domein is dit niet het geval. Er is geen of slechts minimale controle over het apparaat, over het besturingssysteem en over het netwerk, vanaf het moment dat de gegevens het overheidsnetwerk verlaten en via de publieke datanetwerken getransporteerd worden. Dit levert een spanningsveld op met betrekking tot informatiebeveiliging, vooral in relatie tot de BIO.



49 https://www.noraonline.nl/wiki/BIO_(Baseline_Informatiebeveiliging_overheid)

Naast de BIO zijn er nog diverse andere kaders en handreikingen die relevant zijn bij de te nemen maatregelen rondom informatiebeveiliging. Deze kunnen per overheidsorganisatie verschillen. Voor de sector Rijk zijn dit bijvoorbeeld:

- Algemene Verordening Gegevensbescherming (AVG)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR) 2007
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIR-BI)
- NEN-ISOSEC 27001
- NEN-ISOSEC 27002
- Nederlandse overheid Referentie Architectuur (NORA) IB-Katern
- CIP-publicatie “Grip op Secure Software Development (SSD) Beveiligingseisen voor mobile apps”[50]
- NCSC publicatie “ICT-beveiligingsrichtlijnen voor mobiele apps”[51]

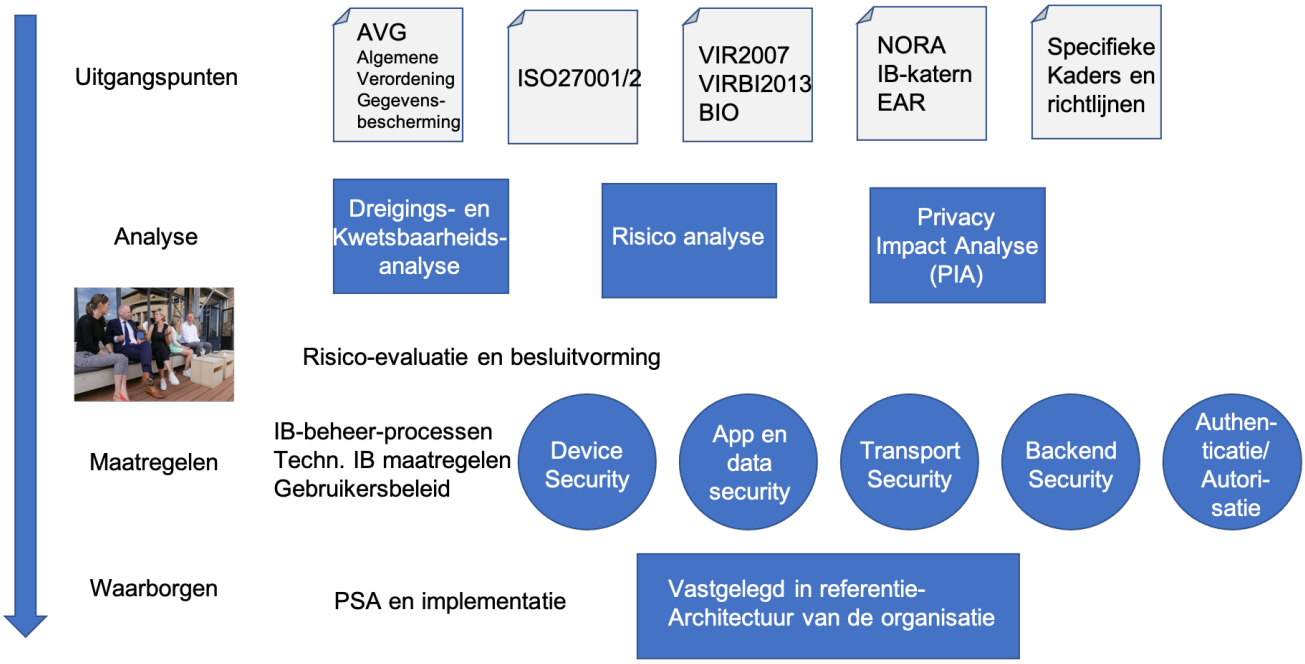
10.2 Maatregelen op basis van een risicoanalyse

De opdrachtgever van de app bepaalt op basis van een risicoanalyse hoe gegevens beschermd dienen te worden en waartegen. Op basis van deze analyse kan, bij voorkeur in samenwerking met de leverancier(s) van de app en/of andere ICT-voorzieningen, de juiste set van de benodigde maatregelen worden vastgesteld. Vragen die belangrijk zijn in dit traject:

1. Hoe belangrijk/vertrouwelijk is de informatie die in een app wordt verwerkt of gepresenteerd?
2. Wie is eigenaar van deze informatie?
3. Welke risico’s zijn er?
4. Welke aanvullende wettelijke of andere regelingen zijn op deze gegevens of de verwerking ervan van toepassing?
5. Op welke platformen draait de app? Wie is de eigenaar van deze apparaten?

50 https://www.cip-overheid.nl/media/1103/20160225_grip_op_ssd_mobile_apps_beveiligingseisen_v100.pdf
51 https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-mobiele-apps

In de volgende afbeelding wordt dit proces weergegeven:



Er zijn drie gouden regels die gelden bij het gebruik van apps die privacygevoelige of andere vertrouwelijke gegevens bevatten. Het verdient aanbeveling om deze regels actief mee te delen aan de gebruiker, bijvoorbeeld door een informatie- of gebruiksvoorwaardenmededeling bij het eerste gebruik van een app te tonen,met daarin het volgende:

1. Gebruik altijd de originele software op het apparaat en de meest recente versie daarvan (besturingssysteem).
2. Gebruik altijd de officiële appstore van het platform of gebruik bij apps voor intern gebruik de interne Enterprise App store of distributievoorzieningen van de eventuele EMM/UEM[52]-tooling.
3. Beveilig de toegang tot het apparaat (met bijvoorbeeld een toegangscode).

Bij het gebruik van apps binnen de eigen bedrijfsomgeving kunnen meerdere maatregelen worden getroffen om de veiligheid van het gebruikte device te waarborgen. Denk hier aan het gebruik van EMM/UEM-voorzieningen die strikte device policies en bijvoorbeeld een remote wipe kunnen afdwingen en strikte regels rondom toegestane versies van de systeemsoftware. Indien een EMM/UEM wordt toegepast; lever zo mogelijk het apparaat beveiligd uit aan de gebruiker of gebruik OS-specifieke activatievoorzieningen om ongeautoriseerde toegang of aanpassingen te voorkomen.

52 EMM= Enterprise Mobility Management; UEM= Uniform Endpoint Management, zie voor uitleg hoofdstuk 'Beheer en distributie'

Belangrijke uitgangspunten voor beveiliging met betrekking tot apps:

- Publieke apps dienen intrinsiek veilig te zijn; er kan niet worden teruggevallen op MAM, MDM of MIM[53]-hulpmiddelen. Een gebruiker moet er van uit mogen gaan dat de app die hij installeert zonder aanvullende maatregelen of instellingen gebruikt kan worden.
- Maak zo veel als mogelijk gebruik van de voorzieningen van het device en het platform om de beveiliging van apps te verbeteren. Betrek de benodigde IB-maatregelen ook bij een eventuele keuze tussen native, hybride of web apps.
- Versleutel de gegevens. Dit geldt voor zowel de gegevens die op het device opgeslagen worden, als voor het transport tussen de app en de back-end systemen via het netwerk.
- Bepaal de sterkte van de sleutel en de cryptografische algoritmen aan de hand van de gevoeligheid en de levensduur van de informatie.
- Bepaal de maximale footprint van de data op het device. Een zero footprint is een ideaal, maar in de praktijk vaak niet haalbaar. Dit zou betekenen dat een app geen data op een device opslaat. Maak een juiste afweging welke data lokaal op het device opgeslagen moet worden, rekening houdend met factoren als performance, belasting back office en dataverbinding en online- en offlinegebruik.
- Voorzie de app van een ‘data clean up’ functie waardoor de app de data die niet langer benodigd is, actief verwijdert van het device.
- Voor bepaalde informatie of bedrijfsprocessen kan het relevant zijn dat slechts een bepaalde set devices (bijvoorbeeld goedgekeurde of bedrijfseigen toestellen) kunnen worden gebruikt. In dat geval kan device-authenticatie een zinvolle maatregel zijn. Hiervoor worden unieke kenmerken van het apparaat gebruikt zoals een uniek identificatienummer of geïnstalleerde certificaten.
- Voor apps die met privacygevoelige informatie werken is het belangrijk om de toegang tot de app af te schermen en niet te vertrouwen op de afscherming van het device. Denk hierbij aan een toegangscode of vingerafdruk voor toegang tot de app. Dit is vooral bescherming tegen medegebruikers van het device bij dagelijks gebruik en niet tegen compromittering en/of hacken van het device.
- Toegang tot privacygevoelige gegevens vereist een afdoende vaststelling van de identiteit van de gebruiker. Kies hiervoor het meest geschikte middel binnen de vigerende authenticatiemethoden. Adopteer tijdig nieuwe authenticatiestelsels wanneer deze voor de doelgroep beschikbaar komen.
- Gebruik voor publieke apps waarvoor authenticatie noodzakelijk is, bij voorkeur de DigiD-app of de authenticatiemiddelen uit het eHerkenningsstelsel. De DigiD-app biedt een mogelijkheid voor apps om te authenticeren voor de diensten die de app gebruikt. Vereiste is wel dat de koppeling met DigiD vanuit de dienst gebaseerd is op SAML. De authenticatie van DigiD-app is voor toegang tot een dienst en niet voor toegang tot de app, maar kan daar natuurlijk ook mee gecombineerd

53 MAM = Mobile Application Management; MDM = Mobile Device Management; MIM = Mobile Information Management, zie voor uitleg hoofdstuk ‘Beheer en distributie’.

worden in online scenario's, zodat gebruikers niet met meerdere authenticaties worden geconfronteerd.

- Denk na over de data die een app op het device bewaart in relatie tot voor de devices gebruikte backup strategie. Mag deze data wel of niet in een backup meegenomen worden en waar kan deze dan terecht komen? Backups kunnen lokaal gemaakt worden (via een USB-kabel) of naar de cloud.
- Bouw echtheidskenmerken in. Apps worden steeds vaker nagemaakt of gemanipuleerd. Het is erg moeilijk om een nagemaakte app van een echte app te onderscheiden of om maatregelen tegen niet-authentieke apps te ondernemen. Een enterprise app die in de appstore staat zou bijvoorbeeld nagemaakt kunnen worden om accountgegevens te kunnen verkrijgen.
- Gebruik geregistreerde beeldmerken zoals het (Rijks)overheidslogo (het blauwe lint) op essentiële plaatsen in de app (zie het hoofdstuk 'User experience'). Onrechtmatig gebruik van een dergelijk beeldmerk vormt een solide juridische basis om zaken uit de de publieke app stores te laten verwijderen.
- Scan regelmatig de diverse publieke appstores op mogelijke onrechtmatige varianten van de app. Dit scannen kan een handmatig of geautomatiseerd proces zijn, afhankelijk van de geïdentificeerde risico's.
- Definieer lifecyclemanagement voor bedrijfsdevices. Devices kennen vaak maar een beperkte support periode door de fabrikant m.b.t. levering van OS-updates en security-patches. Zorg er voor dat alle actieve devices binnen de support van de fabrikant vallen.
- Bij het gebruik van AI kunnen andere soorten aanvallen dan bij traditionele software onstaan. Er kunnen aanvallen plaatsvinden die bijvoorbeeld de uitkomst van een beeldherkenning systeem beinvloeden en daarmee de uitkomst van een beslissing veranderen[54].

54 www.theverge.com/2019/4/23/18512472/fool-ai-surveillance-adversarial-example-yolov2-person-detection

15 Beheer en distributie

Het beheer van en de distributie van mobiele apps zijn op een aantal punten anders dan het beheer van traditionele applicaties op een vaste werkplek. Tegelijkertijd zien we de ontwikkeling om het beheer van de vaste werkplek en mobiele apparaten zo uniform mogelijk te organiseren. Na de introductie van Enterprise Mobility Management (EMM) suites die het mogelijk maken om apps, mobiele apparaten, draadloze netwerken en aanverwante services te managen, is er nu de trend naar Uniform Endpoint Management (UEM) . Wat betreft de (door)ontwikkeling van apps, de gebruikte EMM of UEM suites en het distributiekanaal, kunnen keuzes worden gemaakt. Deze zijn in dit hoofdstuk beschreven. Verder heeft de keuze voor publieke apps of interne overheidapps impact op de te volgen beheerstrategie.

11.1 (Door) ontwikkelen van apps

Specifiek voor de (door)ontwikkeling van apps is het snel en frequent opleveren van nieuwe versies naar de productieomgeving. Een DevOps werkwijze, waarbij beheer en ontwikkeling samen verantwoordelijk zijn voor de werking en de ontwikkeling van een dienst, is hiervoor heel geschikt.

Om de integriteit van de app in het overheidsdomein te waarborgen is het ondertekenen met een door de overheid uitgegeven of organisatie specifiek certificaat essentieel. Bij het ondertekenen wordt een legitieme status toegekend aan de app waarmee deze “integer” kan worden aangeboden aan de eindgebruiker.

Laat de app niet ondertekenen door een commerciële partij, dit maakt het beheer complexer en is verwarrend voor de gebruiker. Uitzondering kan gelden voor public apps die door externe partijen zijn ontwikkeld in opdracht van de overheid. Als zo’n app in beheer blijft bij de externe ontwikkelaar dan kan je ervoor iezen om die te laten signen door die externe partij. Anders heb je veel beheerslast (elke nieuwe release overdragen en signen door overheidspartij) en moet je vertrouwen hebben in de kwaliteit/veiligheid van de app omdat jouw naam er aan hangt (imago risico)

Biedt apps aan in vertrouwde overheidsAppStores of met een label van de overheid in publieke stores. Voor Android apps is er sinds kort geen mogelijkheid meer om in eigen app store te hosten maar moet je de app via de Managed Google Playstore aanbieden. Apple gaat ook die kant op is de verwachting. Dit heeft gevolgen voor de veiligheid i.v.m. het aanleveren van de app code aan Google (en later Apple)

Voor het beheer van certificaten (Apple) en Keystores (Android) is het aan te raden om hier gedegen beheer voor in te richten om te voorkomen dat certificaten kwijtraken, waardoor updates van apps niet uitgevoerd kunnen worden. Tevens moet ervoor gewaakt worden dat certificaten in handen vallen van derde partijen.

Voor het beheer van gepubliceerde apps in enterprice AppStores is het aan te raden om een agenda in te richten voor het opnieuw tekenen van apps. De distributieprofielen (van Apple) zijn op dit moment maximaal 11 maanden geldig. Als de app niet tijdig getekend en opnieuw gedistribueerd wordt, zal deze niet meer werken.

Om apps vitaal en veilig te houden is het advies om een App minimaal twee maal per jaar op te (laten) bouwen, ook als er geen functionele wensen bestaan op dat moment. Op die manier blijft de app compatabel met de actuele versies van het besturingssysteem, gebruikte SDK's en alle componenten waaruit de app is opgebouwd.

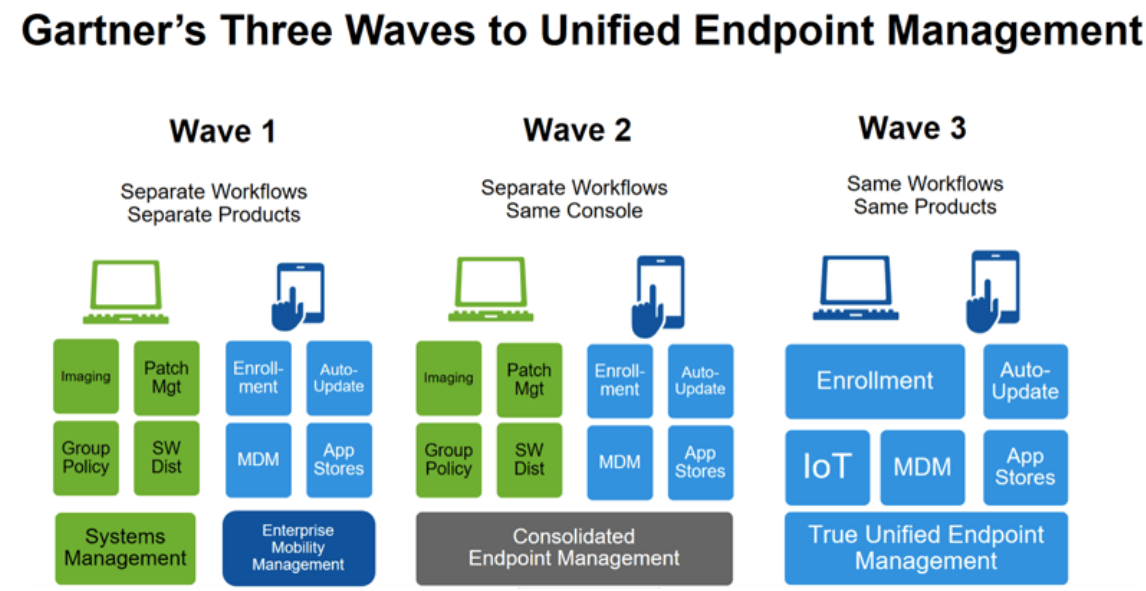
11.2 Unified Endpoint Management (UEM)

Voor IT-managers betekent de toename van (mobiele) devices op en buiten kantoor dat ze meerdere MDM-systemen, EMM-platforms en client managementtools in de lucht moeten houden. Tegelijkertijd moeten ze oplossingen bedenken voor de continue stroom aan nieuwe devices, besturingssystemen, apps en malware-bedreigingen die digitale transformatie met zich meebrengt . Wordt daar niet adequaat op geacteerd, dan leidt dat vroeg of laat tot schade en verlies van data. Onder de nieuwe Europese privacywet AVG kan een datalek fikse boetes opleveren.

Het gebruik van een UEM oplossing kan een mogelijke oplossing zijn voor deze uitdagingen. Unified Endpoint Management (UEM) is de verzamelnaam voor een IT oplossing die de mogelijkheid geeft om een grote verscheidenheid aan apparaten met verschillende verschijningsvormen en besturingssystemen zoals PC's en laptops, tablets en smartphones, en ook wearables en Internet of Things (IoT) eindpunten centraal te beheren. Veelal bestaat de oplossing uit de volgende onderdelen:

- Mobile Device Management (MDM);
- Mobile Application Management (MAM);
- Mobile Content Management (MCM);
- Mobile Identity & Access Management (MIM).

De afgelopen jaren is de scope van de beheer oplossingen steeds meer gericht op een integrale beheeromgeving voor alle type devices en operating systemen. Waar tot 5 jaar gelden vaak meerdere oplossingen naast elkaar nodig waren om Windows en Android en macOS te beheren is dat tegenwoordig mogelijk vanuit 1 oplossing.



Mobile Device Management (MDM) draait om het beheer van alle mobiele apparaten die binnen een bedrijf of organisatie in omloop zijn. Het beheer van de instellingen, gebruikersrechten en beveiligingsbeleid gebeurt allemaal vanaf één cenraal punt. Dit stelt de organisatie in staat zowel privé als vanuit het bedrijf verstrekte apparaten te laten vergrendelen of te wissen om zodoende de beveiliging van data mogelijk te maken.

MDM-gebaseerde oplossingen hebben de volgende beperkingen:

- **Beperkt bereik;** via MDM kunnen alleen apps aan de interne medewerkers, van het eigen verzorgingsgebied worden gedistribueerd, niet aan de burger. MDM wordt meestal ingezet voor apparaten die eigendom zijn van de organisatie. Tenslotte kan er slechts één organisatie het device managen. Dit is een beperking, in het geval dat rijksambtenaren bij meerdere ministeries werkzaam zijn en in het geval van apps die Rijksbreed aangeboden moeten worden.
- **Gebrek aan beheerfuncties voor apps;** de app-distributie functies in sommige MDM oplossingen zijn geschikt voor relatief simpele apps en niet geschikt voor complexe omgevingen waar bijvoorbeeld gebruikersgroepen over een eigen set aan apps moeten beschikken.

Mobile Application Management (MAM) richt zich op het beveiligen en beheren van apps en gegevens binnen de app (data at rest) en de verbinding tussen de app en het informatiesysteem (data at transit) , los van het device en is geschikt voor privé-apparaten van medewerkers. Via een MAM platform kunnen apps ook gedistribueerd worden op elk apparaat, ongeacht of een app wordt beheerd via een MDM systeem. Een nadeel is dat MAM zonder MDM geen tegenwicht biedt aan de kwetsbaarheden van het operating system, wat alsnog kan leiden tot kwetsbare apps. MAM wordt dan ook vaak in combinatie met MDM toegepast. MAM biedt verder de mogelijkheid om diensten te leveren buiten het eigen verzorgingsgebied van de IT-leverancier en rijksbrede apps te ontwikkelen en

te distribueren. Binnen deze “app centric” benadering moet een goede MAM oplossing de volledige app-levenscyclus ondersteunen met o.a. de volgende functies:

- Het toevoegen van apps aan het systeem (“app-onboarding”);
- Het inspecteren van apps om ervoor te zorgen dat ze veilig zijn (“app-inspectie”);
- Het beveiligen van apps met maatregelen vanuit opgesteld beleid (“app-bescherming”);
- Het verspreiden van apps naar alle gebruikers (“app-distributie”);
- Bepalen of apps worden gebruikt en het verkrijgen van de gebruikerrecencies (“app-analytics”);
- Onderhouden apps op regelmatige basis (“app-updates”);
- Per app VPN-functionaliteit;
- Het intrekken(uitfaseren) van verouderde apps.

Mobile Content Management (MCM): Het idee achter MCM is het veilig kunnen aanbieden van bedrijfsdata op mobiele apparaten. In de hedendaagse UEM platformen is MCM vaak geïntegreerd. Hierbij kan men denken aan file sharing van zowel data in de cloud als data binnen bestaande domeinen (bijvoorbeeld netwerk fileshares), gepresenteerd naar een mobiele front end, of het kunnen benaderen van SharePoint sites of home directories. Er zijn reeds producten op de markt die interfaces hebben naar bekende Enterprise Content Management oplossingen zoals Filenet, IBM connection en Hummingbird. MCM oplossingen maken gewoonlijk gebruik van een veilige container rond gevoelige data, deze is encrypted en alleen geautoriseerde gebruikers kunnen er bij. Om MCM optimaal in te zetten, moet identity management hier onderdeel van uit maken.

De laatste jaren komen er steeds meer Content Collaboration Platformen op de markt, Deze oplossingen bestaan uit een verzameling van tools en hulpmiddelen die zorgen dat medewerkers op elk gewenst moment toegang hebben tot (gedeelde) content en veilig kunnen samenwerken door gebruik te maken van geintegreerd digital rights management (DRM) protectie op bestanden. Hierdoor blijft de informatie veilig, ongeacht de locatie, zelfs als de informatie zich buiten de firewall van de organisatie bevindt. Door het analyseren van monitoringinformatie kunnen verdachte patronen herkend worden en eventuele veiligheids lekken achterhaald worden. Zeker in het kader van EU’s General Data Protection (GDPR) kunnen deze systemen een toegevoegde waarde hebben.

Mobile Identity Management (MIM): MIM houdt zich voornamelijk bezig met het waarborgen dat de werknemers het juiste niveau van machtigingen krijgen tijdens de toegang tot bedrijfsgegevens. Mobile Identity Management beheert toegangscontrole met Enterprise Single sign-on mogelijkheden, multi-factor Authentication etc.

Unified Endpoint Security: Als gevolg van de toename van mobile devices en evengrote toename van bedreigingen is de noodzaak van integrale beveiling op de devices toegenomen. De meeste leveranciers hebben een additionele oplossing ontwikkeld bovenop het UEM platform met additionele beveiligings mogelijkheden zoals, endpoint detection, endpoint protection en mobile Threat defense.

Deze technologie werkt vaak op basis van artificial intelligence(AI) en machine (ML). Het doel is het voorkomen, detecteren en reageren op eventuele bedreigingen.

11.3 Keuze voor een EMM/UEM oplossing

Er zijn verschillende redenen om een UEM oplossing te gebruiken zoals het op afstand willen beheren van apparaten, het afdwingen van het gebruik van een wachtwoord op apparaten en de distributie van apps. Deze oplossing wordt veelal gebruikt in het geval dat er sprake is van bedrijfsapps voor interne medewerkers die een hoog beveiligingsrisico hebben. Indien burgers de doelgroep vormen, is deze beheeroplossing niet toepasbaar. De volgende aspecten zijn relevant bij de keuze voor een UEM oplossing.

- **Compleetheid.** Een goede UEM oplossing biedt niet alleen MDM-mogelijkheden om apparaten te beveiligen en te beheren, maar zorgt ook voor het distribueren van apps en het beheren en beveiligen via MAM en functionaliteit voor identiteits- en toegangscontrole.
- **Volwassenheid.** UEM zelf is inmiddels een mainstream product en vormt vaak een onderdeel van de bredere dienstverlening. Dit houdt in dat een volwassen UEM oplossing binnen één overkoepelende beheerconsole te managen is. Let er op dat de leverancier een roadmap voor de toekomst heeft klaarliggen en eerdere acquisities om de UEM functionaliteit aan te vullen, goed heeft geïntegreerd.
- **Gemakkelijk uit te rollen.** De eenvoud in deployment verschilt tussen de diverse aanbieders. Dit is van belang omdat de behoeften per organisatie verschillen en er ook op het niveau van teams en individuen andere eisen kunnen gelden. Dat vraagt om een brede inzet van verschillende policies en tools en - dus - om een flexibele oplossing.
- **Schaalbaarheid.** Zowel de werkgerelateerde inzet van mobiele apparaten als het aantal apparaten per werknemer groeit. Een UEM oplossing moet in de toekomst kunnen meeschalen met de groei van het aantal apparaten. Let daarbij op de kosten.
- **Licentiestructuur**. Een pakket moet de keuze bieden tussen een user- of een device-licentiestructuur. Kies de licentiestructuur die het beste aansluit bij het bedrijfsmodel. Vanwege de toename van het aantal mobiele apparaten per persoon is de user based licentiestructuur vaak het efficiëntste.
- **Reputatie leverancier.** Hoewel een aantal UEM leveranciers inmiddels een goede naam heeft opgebouwd, zijn er flink wat spelers die pas net komen kijken en nog geen of weinig cases kunnen laten zien. Kijk daarom goed naar de reputatie van het bedrijf, naar de branches waarin ze klanten bedienen en naar de ervaringen van deze partijen. Een

mogelijke bron is het Magic Quadrant dat Gartner ieder jaar publiceert. Een multilayer concept is in sommige gevallen een goede oplossing om minder afhankelijk te zijn van één leverancier.

- **On-site versus cloud**. In lijn met de algehele transitie naar de cloud hebben veel leveranciers tegenwoordig zowel een oplossing on-site als een oplossing waarbij het platform als een dienst uit de cloud afgenomen kan worden. Iedereen zal een eigen afweging moeten maken d.m.v. een riscicoanalsye of deze in lijn zijn met de security kaders en dit tot de mogelijkheden behoort. Het afnemen van een cloudoplossing heeft als grote voordeel dat het beheer van de infrastructuur niet intern gedaan hoeft te worden en de focus kan liggen op het configureren en implementeren. De ervaring leert dat de implementatie en Lifecyclemanagement van de infrastructuur veel tijd en kennis behoeft.

11.4 Aantal “best practices”

Een aantal “best practices”op het gebied van UEM:

- **Beveiliging versus gebruiksvriendelijkheid;** zorg dat de gebruiksvriendelijkheid en beveiliging in evenwicht zijn. Als de policies te strak worden ingesteld, gebruiken medewerkers de functionaliteiten niet en gaan ze er omheen werken. Door gebruik te maken van de laatste technologieën, kan de gebruiksvriendelijkheid verbeterd worden. De mogelijkheid om data te ontsluiten via vingerscan bijvoorbeeld, verhoogt de gebruikersbeleving aanzienlijk. Het zal per organisatie echter bekeken moeten worden of deze technieken toegepast kunnen worden in verband met het vigerende beveiligingsbeleid. Raadpleeg de zogenaamde inzet adviezen van het NBV[55] over de inzetbaarheid van UEM omgevingen binnen de (Rijks)overheid. Houd tenslotte ook rekening met de dataclassificatie van de informatie bij de keuze van de UEM oplossing.
- **Toegangscontrole;** beperk het gebruik van verschillende wachtwoorden voor apps tot een minimum. Sommige UEM leveranciers bieden de mogelijkheid om apps binnen de beveiligde omgeving met hetzelfde wachtwoord te beveiligen. De beste beleving wordt gerealiseerd als Single sign-on (SSO) ingeregeld kan worden voor de toegang tot apps. Aangetekend kan nog wel worden dat de toegang tot data in systemen in de back-end niet door een UEM geregeld kan worden. Het slot op de deur hiervoor vereist wel een afzonderlijke autorisatie.
- **Beheerorganisatie;** de ondersteuning van mobiele diensten is wezenlijk anders dan de ondersteuning van bijvoorbeeld Windows-werkplekken. Indien de gebruiker een probleem heeft met zijn device of app is remote ondersteuning lastig. Het is dan ook aan te bevelen om een service desk in te richten voor ondersteuning voor mobiele apparaten

55 https://www.aivd.nl/onderwerpen/informatiebeveiliging/inhoud/beveiligingsproducten/inzetadviezen

of deze te integreren met de bestaande. Storingen aan mobiele diensten kunnen complex zijn. De dienst is afhankelijk van vele ICT-componenten en vaak verschillende ondersteunende beheerteams. Mobility-diensten vereisen een interne keten gestuurde aanpak. Het is dan ook aan te bevelen de diverse mobility-disciplines in één afdeling onder te brengen (bijvoorbeeld in een mobile competence center).

- **Uitrol mobiele apparaten;** het uitleveren van mobiele apparaten aan de eindgebruikers is een tijdrovende klus. De gebruiker speelt hier een essentiële rol, omdat er een persoonlijk account nodig is om apps van de verschillende leveranciers te installeren vanuit de verschillende app stores. Bij veel organisaties moet de gebruiker daarom zelf de configuratie van het device uitvoeren. Als de uitrolprocedure niet gebruiksvriendelijk is, geeft dit in de praktijk veel problemen en veel druk op de beheerorganisatie en/of de servicedesk.
- **Automatiseren uitrol;** er zijn momenteel oplossingen beschikbaar om de uitrol te verbeteren en de doorlooptijd van het uitrol-proces te verkorten, bijvoorbeeld het Apple Business Manager Portal (BMP, voorheen Deployment Enroll Program (DEP)) of het Knox Mobile Enrollment Program van Samsung. Recent heeft Google “Zero touch enrollment” geïntroduceerd. Alle oplossingen zijn erop gericht om de uitrol van het MDM en de apps sneller te laten verlopen met minimale inspanning van de gebruiker. Als BMP samen met het Volume Purchase Program van Apple gebruikt wordt , is het mogelijk om apps zonder het gebruik van een Apple-ID of Google account te installeren.
- **Kennis delen;** de kennis in de markt van UEM oplossingen is schaars. Ongeacht welke oplossing gekozen wordt, is het beschikbaar hebben van kennis binnen de organisatie van essentieel belang. Denk hierbij ook aan workshops en trainingen van gebruikers om de adoptie van mobiele diensten te verbeteren.

11.5 Distributiekanalen

Er zijn verschillende vormen van distributie voor apps. Welke vorm gebruikt kan worden hangt sterk af van de doelgroep van de app. Er is de afgelopen jaren het nodige veranderd en trend is dat Apple en Google steeds meer de regie pakken over de manier waarop de distributie gedaan dient te worden.

Publieke apps voor burgers

Apps voor burgers en bedrijven dienen voor iOS in de Apple AppStore en voor Android in de Google Play store geplaatst te worden. Distributie op deze manier zorgt dat gebruikers hun toestel veilig kunnen houden, geen jailbreak of rooten en geen apps uit onbekende bronnen aanzetten. Voor Android toestellen van Huawei waar de Google Play diensten niet beschikbaar zijn kan Huawei AppGallery store gebruikt worden. Vaak zal dit een aparte app zijn die gebruik maakt van de alternatieve diensten van Huawei. Voor apps van de Rijksoverheid wordt aangeraden de Rijksoverheid accounts te gebruiken welke door het Apploket van Dictu worden beheerd. Apple en Google publiceren de apps niet ongezien maar doen eerst een review op de app of deze voldoet aan de eisen van de stores. Deze eisen worden regelmatig aangepast. Een belangrijke eis is dat er voor het review proces test accounts beschikbaar moeten zijn. Voor apps die DigiD vereisen heeft de DigiD-app een demo optie die hiervoor gebruikt kan worden.

Enterprise apps

Enterprise apps zijn apps die niet voor iedereen te gebruiken zijn. Apple en Google zien deze apps liever niet standaard in de publieke store lijsen. Enterprise apps worden daarom via de enterprise opties van Apple en Google verspreid. Voor apps die op een beheerd toestel van medewerkers moeten komen wordt gebruik gemaakt van Apple Business Manager en Managed Google Play in combinatie met een EMM oplossing. Voor iOS is het nog wel mogelijk om zelf enterprise apps met een EMM oplossing direct intern te distributeren alleen zit daar het nadeel aan dat de app elk jaar een update moet krijgen vanwege de beperkte geldigheid van de provisioning profiles. Voor apps die op niet beheerde toestellen geinstalleerd moeten worden kan nu nog de normale Google Play store worden gebruikt en biedt Apple de optie van custom apps aan. Deze laatste kunnen via de Rijks App Store worden aangeboden. De Rijks App Store is in beheer bij het Apploket van Dictu.

Distributie naar testers

Tijdens de ontwikkeling van apps dienen deze natuurlijk ook getest te worden. Hiervoor kan gebruik gemaakt worden van de faciliteiten die Apple en Google bieden. Apps kunnen in de Apple AppStore via Testflight en bij Google Play in de test-tracks aangeboden worden aan testers en de app kan na succesvolle testen en goedkeuring gepubliceerd worden.

11.6 Beheer van mobiele apparaten en apps

De controle over mobiele apparaten is beperkt en niet te vergelijken met het beheer van de traditionele werkplek.

Afhankelijkheid OS-updates; bij mobiele platformen ontbreekt de controle over het tijdstip dat updates van het onderliggende operating system vanuit de leverancier beschikbaar gemaakt worden. Apple biedt momenteel een mogelijkheid om updates van het operating system uit te stellen of te pushen via Apple Busininess Manager. Samsung kan tegenwoordig ook updates pushen of tegenhouden via het Enterprise Firmware Over The Air(E-Fota) systeem. Apple publiceert de updates zonder aankondiging, maar wel met een regelmatige frequentie. Android kent een directe afhankelijkheid van de verschillende device leveranciers, waardoor de nieuwste versies van Android niet op alle hardware beschikbaar komt. Het effect is dat er meerdere versies van het operating system aanwezig zijn binnen de installed base. Het advies is om door middel van het instellen van compliancy rules gebruikers te dwingen om de laatst beschikbare versie voor het device te installeren of een minimum versie in te stellen. Zorg verder dat lifecyclemanagement goed is geregeld.

Monitoring; een actueel beeld van gebruik/user metrics, foutcontrole, performance en feedback is van belang voor goed app-management. Het brengt de volwassenheid van de app in kaart en vormt de verdere doorontwikkeling van de functionaliteit. Aan de platformkant kan gebruik gemaakt worden van tooling als MS App center, TestFlight, Firebase. Voor het opdoen van gebruikerservaring kan juist gebruik gemaakt worden van “inApp” feedback opties of de review mogelijkheden die de app store zelf levert. Bescherming van persoonsgegevens moet wel goed ingeregeld worden.

Eigenaarschap app; apps kennen vaak vele wijzigingen in functionele eisen en wensen van de opdrachtgever. Met daarbij de vele updates van de leveranciers op operating system niveau en gebruikte SDK’s en andere standaard componenten is het van belang snel en adequaat op veranderingen te kunnen reageren. Belangrijk hierbij is om de kwaliteit te handhaven. Dit betekent dat het onderhouden van de app een belangrijk proces is. Als dienstverlener is het belangrijk om goede afspraken te maken met de app- eigenaar. Deze is immers als opdrachtgever in de lead om op tijd een nieuwe versie te initiëren. Functioneel beheer en lifecyclemanagement dient ingericht te zijn. Als de app niet in eigen beheer is, is goede afstemming met de derde partij van grootbelang om de dienstverlening te kunnen garanderen. Zeker nu steeds meer primaire processen mobiel aangeboden worden.

16 12 Betrokken Partijen

Bij de totstandkoming van dit document zijn de volgende partijen betrokken opgedeeld en schrijvers en reviewers.

Namen	Schrijvers	Rol bij app ontwikkeling	Expertise & Verdere bijz.
Belastingdienst **Jeroen Dijkgraaf** **Coördinatie & redactie** **Leendert Versluijs (schrijver)**	j.dijkgraaf@belastingdienst.nl l.versluijs@belastingdienst.nl	Contactpersoon Belastingdienst Klant Domein Mgr. & PM Digitale Interactie Ontwikkelt voor burgers, bedrijven & rijksambtenaren native apps.	Mobile Account Mgt. & Portfolio Mgt & Strategische personeels-planning Mobile architectuur, Ontwikkel proces, Security, User Interface Design, Xamarin, MobileIron
DICTU **Ronald Heukers (schrijver)** **Leon Boon (schrijver)**	w.j.r.heukers@dictu.nl l.boon@dictu.nl	Contactpersoon Referentiearchitectuur Sr. Mobile Developer Ontwikkelt voor burgers, bedrijven & ambtenaren native apps	App architectuur, security, XenMobile Artificial Intelligence in de mobiele context Native app ontwikkeling (iOS + Android) en distributie van apps
Defensie **Allard Zomer (schrijver)**	aj.zomer@mindef.nl	Ontwikkelt voor burgers & Defensieambtenaren hybride en web apps. Adviseur mobiele toepassingen	App architectuur, Ontwikkel proces
SSC-ICT **Marco Knorren** **Marco Janssen (review)** **Martin Krouwer (review)**	marco.knorren@minbzk.nl Marco.janssen@minbzk.nl Martinkrouwer@minbzk.nl	Verantwoordelijk voor overkoepelende strategie rondom hybride werken, beheer van (mobiele) werkplekken meerdere ministeries, regie op Appontwikkeling en distributie op diverse platformen (iOS, Android, Windows) apparaten	Beheer moderne (mobiele)werkplek met Blackberry Unified endpoint management Appdistributie
JIO (Justitie ICT Organisatie) **Dennis Brocker** **Frank van Hof** **Michael Ramlal (schrijvers)**	d.brocker@dji.minjus.nl f.v.hof@dji.minjus.nl m.ramlal@dji.minjus.nl	Sr. Adviseur informatiebeveiliging en privacy (qwalty assurance) Ontwikkelt voor rijksambtenaren, burgers en justitiabelen hybride & native apps.	Quality assurance en ethicak hacking HTML5, Javascript, Apache Cordova, UX Design, Vue.js Typescript beveiliging, Mobile Iron
Politie **Eddy Spreeuwers (review)**	eddy.spreeuwers@politie.nl	Ontwikkelt voor medewerkers & burgers hybride & native apps.	App architectuur, Ontwikkel proces, Security, User Interface Design, Xamarin, MobileIron