Indieningsformulier oplossingen
Innovatiebudget NL DIGIbeter - 2019

Met dit formulier kunnen overheidsmedewerkers oplossingen voor het NL DIGIbeter innovatiebudget voorstellen. Informatie over het innovatiebudget, inclusief deadlines en selectiecriteria is te vinden op digitaleoverheid.nl/innovatiebudget.

Heb je een voorstel voor een goede oplossing? Vul dit formulier volledig in en mail het vóór de deadline naar Team Innovatiebudget, [redacted], liefst met '[Voorstel oplossing]' in het onderwerp. Kijk eerst zelf nog even of het voorstel aan de (harde) criteria voldoet. Neem voor vragen contact op met het team, via hetzelfde adres.

Succes!

1 Algemene gegevens

Oplossingstitel	Telefonische identificatie
Korte omschrijving oplossing	Proof of concept voor telefonische multifactor authenticatie op basis van open source software
Indienende organisaties (inclusief welke regie voert)	Gemeente Nijmegen (regie) Gemeente Arnhem Hogeschool Arnhem Nijmegen Radboud Universiteit Coöperatie VGZ UA Vtel telecom
Contactpersoon (verantwoordelijke) **Naam**	[redacted]
Telefoonnummer	[redacted]
Email	[redacted]
Aansluiting bij NL DIGIbeter	Toegankelijkheid, begrijpelijk en voor iedereen: - Onderzoek naar digitale identificatie en verificatie - Samenhangende aanpak voor digitale inclusie - Overheidsbreed maken we gebruik van de principes van 'Gebruiker Centraal' - Ontwikkeling gebruiksvriendelijke digitale producten - Verdere ontwikkeling DigiD, en toelaten één of meerdere eID-middelen - Wederzijdse erkenning elektronische identificatie - Testen van diverse nieuwe digitale identiteitstoepassingen - Stimuleren van het vrijgeven van eigen software als open source software
Voorgenomen eigen bijdrage (we verwachten 20% cofinanciering)	€ 24.000,- inzet in uren
Omschrijving van eventuele bijlagen (bijvoorbeeld probleemanalyse, kosten-batenanalyse, partnerverklaringen, PvA)	-

2 Overzicht oplossing

2.1 Aanleiding en oplossing

Aanleiding

Er zijn groepen mensen in de samenleving die om verschillende redenen vaker dan anderen aankloppen om hulp of diensten, bijvoorbeeld bij zorgverleners, de verzekeringsmaatschappij of de gemeente. Het betreft vaak mensen die van een pensioen, uitkering of bijstand afhankelijk zijn, of die een chronische ziekte of beperking hebben en daardoor veel voorzieningen aanvragen en facturen indienen. Steeds vaker moeten die hulp of diensten digitaal aangevraagd en afgenomen worden. Daarvoor moet men zich online digitaal kunnen identificeren.

Het valt op dat naast digitaal contact ook veel vragen over diensten per telefoon worden gesteld worden (zie cijfers onder 2.2). Bellers geven vaak de voorkeur aan dat contactkanaal omdat het laagdrempelig is en je makkelijk door kunt vragen op de informatie die je krijgt. Voor een relatief groot deel van de 'afnemers' van diensten is telefonisch contact veel toegankelijker dan digitaal contact via teksten en formulieren op het scherm van computer of smartphone, bijvoorbeeld omdat ze beperkte digitale vaardigheden hebben, of moeite hebben met lezen en begrijpen van tekst. Ook bij telefonische dienstverlening moeten de bellers zich kunnen identificeren, omdat er privacygevoelige persoonlijke gegevens uitgewisseld worden, bijvoorbeeld over financiële en medische zaken.

Er is op het moment geen betrouwbare en veilige manier van telefonische identificatie. Daardoor moeten de dienstverlenende professionals melden dat zij de gevraagde gegevens niet mogen verstrekken en de bellers doorverwijzen naar een website of via een terugbelverzoek naar een behandelaar. Dit leidt tot negatieve gebruikservaringen bij de bellers, wat ten koste gaat van de beoogde kwaliteit van dienstverlening. Soms wordt er in goed vertrouwen aangenomen dat de bellers inderdaad degene zijn die zij zeggen te zijn, als zij een DigiD, BSN of klantnummer kunnen noemen of een 'geheime vraag' kunnen beantwoorden. Deze oplossing van het identificatieprobleem voldoet niet aan de basiseisen van zorgvuldige en veilige gegevensbescherming, die vastgelegd zijn in de AVG.

Voor de verdere ontwikkeling van (digitale) dienstverlening is het belangrijk dat er aan een oplossing gewerkt wordt voor het probleem van identificatie in telefoongesprekken. In het voorgestelde project onderzoeken en ontwikkelen we telefonische identificatie in de publieke sector en richten we ons op casussen uit het sociale domein en de zorg. Maar de vraag naar betrouwbaar, veilig en makkelijk digitaal identiteitsmanagement speelt in alle vormen van dienstverlening, óók in de private sector van bijvoorbeeld telecomproviders, banken en webwinkels. Dit project is daarom relevant voor veel verschillende maatschappelijke contexten.

Onderzoeksvraag

De vraag in dit project komt van partners uit het door het HAN-CIM opgerichte Netwerk SlimID (zie hieronder). Vier netwerkpartners, namelijk zorgverzekeraar VGZ en de gemeenten Nijmegen en Arnhem en Vtel telecom, hebben het HAN Centrum IT + Media en de Radboud Universiteit gevraagd om voor hen en met hen onderzoek te doen naar de mogelijkheden en beperkingen van IRMA in telefonische dienstverlening waarbij identificatie en authenticatie nodig is. Hun vraag luidt:

Hoe kunnen onze cliënten/inwoners zich veilig, makkelijk en toegankelijk aan de telefoon identificeren als er privacygevoelige informatie wordt uitgewisseld, zoals financiële en/of medische informatie?

IRMA voor veilige, privacy-vriendelijke en gebruiksvriendelijke identificatie

Een mogelijk antwoord op deze vraag komt in de vorm van het identiteitsplatform IRMA. Dit system voor veilige, privacy-vriendelijke en gebruiksvriendelijke identificatie is ontwikkeld door de Digital Security onderzoeksgroep van de Radboud Universiteit (olv prof Bart Jacobs). IRMA is een decentraal, gedistribueerd identiteitsmanagementplatform waarbij de persoonsgegevens en de regie daarover liggen bij de persoon die zich moet identificeren.

IRMA staat voor "I Reveal My Attributes": bij identificatie met IRMA deel je alleen die informatie

(attributen) van jezelf die gezien de situatie en je rol in die situatie noodzakelijk zijn. Je eigen telefoon werkt als een digitaal kluisje. In dit kluisje bewaar je gegevens (attributen) die je bij betrouwbare bronnen (trusted third parties), zoals het gemeentelijk persoonsregister, kan ophalen. Bijvoorbeeld kan je je naam, geslacht, adres en BSN in de IRMA app zetten, en zo een soort digitaal paspoort samenstellen. Niet relevante gegevens uit je app worden hierbij niet gedeeld. Je deelt dus op die manier veel minder persoonsgegevens dan wanneer je je paspoort laat zien, waarop ook voor de situatie irrelevante kenmerken zichtbaar zijn, zoals je geslacht, je uiterlijk, je geboorteplaats en je BSN.

De IRMA-technologie krijgt veel publiciteit en de ontwikkelaars worden met prijzen beloond (o.a. Nederlandse Privacy award 2018, Internet Innovation award 2019). Grote partijen in Nederland onderzoeken op het moment de mogelijkheden en beperkingen van IRMA als een slimme, 'slanke' oplossing bij de uitwisseling van privacygevoelige gegevens op internet. Maar IRMA biedt ook mogelijkheden voor identificatie voor diensten die via de telefoon worden geleverd en afgenomen, en levert dus een concrete oplossing voor het probleem van betrouwbare en veilige manier van telefonische identificatie.

2.2 Behoefte en beleidsverantwoordelijkheid

Beoogde gebruikers

De beoogde gebruikers voor deze oplossing zijn KCC's van overheidsinstellingen, zorgverzekeraars en huisartsenposten. Het geschetste probleem doet zich voor bij alle overheidsinstanties, zorgverzekeraars en huisartsenposten, maar zoals in de aanleiding gesteld, ook in veel andere sectoren.

Omvang van het probleem in de praktijk

Arnhem ontvangt per jaar 180.000 telefoontjes van inwoners en Nijmegen heeft in 2018 213.766 telefoongesprekken met inwoners gevoerd. In naar schatting 60-70 procent van die gesprekken komt informatie aan de orde die vraagt om identificatieplicht, bijvoorbeeld bij gesprekken over belastingen, bijstand en ondersteuning vanuit de WMO en Jeugdwet.

Zorgverzekeraar VGZ heeft in 2018 ruim 2.9 miljoen telefonische contacten gehad waarvan in minstens 90% van de gevallen identificatie nodig is. Verzekerden bellen in bijna alle gevallen over hun persoonlijke situatie en dan is identificatie vereist.

Tot slot verzorgt partner in het Vtel telecom de telefonische bereikbaarheid meer dan de helft van alle huisartsenposten in Nederland. Deze huisartsenposten beantwoorden jaarlijks 15 tot 20 miljoen telefoongespreken waar in 99% van de gevallen vastgelegde identificatie vereist is, aangezien er anders geen medische gegevens mogen worden gemuteerd én de huisartsenpost geen financiering ontvangt van de zorgverzekeraar.

Beoogde oplossing

Een oplossing voor betrouwbare en veilige telefonische identificatie komt in de vorm van de IRMA app. Door vanuit het KCC een bericht naar de IRMA applicatie op de telefoon van de inwoner te sturen, kan de inwoner middels de applicatie geverifieerde identiteitsgegevens op een veilige wijze verstrekken aan de gemeente. Op deze wijze kan de medewerker in het KCC de identiteit vaststellen van de inwoner, waarna persoonlijke gegevens kunnen worden uitgewisseld. Dit proces kan ook geautomatiseerd, voorafgaand aan het gesprek plaatsvinden, zo dat de KCC-medewerker geen tijd kwijt is met het authenticatieproces, maar direct over kan gaan tot de eigenlijke dienstverlening.

Beleidsverantwoordelijkheid

De gemeente is verantwoordelijk voor het uitvoeren van diverse wettelijke taken. In dit project zullen de betrokken partijen zich richten op de taken vanuit het sociaal domein, vastgelegd in de Participatiewet, de Wet Maatschappelijke Ondersteuning, Jeugdwet en de participatiewet.

In 2015 hebben de gemeente deze taken overgenomen met als eis om kwaliteit, de toegankelijkheid

en de betaalbaarheid op peil te houden. Dat kan alleen als mensen en middelen doelmatig en doelgericht worden ingezet, met behoud van de beoogde kwaliteit van dienstverlening. Door telefonische dienstverlening mogelijk te maken, kunnen we de toegankelijkheid verbeteren, de kwaliteit verhogen en de taken betaalbaarder uitvoeren. De kostprijs van een telefoongesprek binnen het KCC zijn +/- €7,-, dit is significant minder dan een huisbezoek of keukentafelgesprek. Volgens gegevens van partner Vtel wordt ongeveer 30% van de tijd in gesprekken met huisartsenposten gebruikt voor identificatie. Als de telefonische identificatie afgehandeld kan worden voordat de beller in gesprek is met de KCC-medewerker, wordt de kostenefficiëntie van telefonische dienstverlening nog verder vergroot.

De zorgverzekeraar voert taken uit in het kader van de zorgverzekeringswet en heeft vanuit deze wet de verplichting om inwoners te voorzien van informatie over de genoten zorg en vragen van inwoners over zorg te beantwoorden. Hiervoor geldt een streng protocol dat wordt getoetst door het Zorgverzekeraars Nederland en de Nederlandse Bank.

2.3 Stakeholders

- *Welke stakeholders zijn er (binnen/buiten indienende organisaties)? Wat is hun relatie met de oplossing? Is er al contact mee? Als hulpmiddel kan onderstaande tabel gebruikt worden.*

Stakeholder	**Belang**	**Belangrijkheid**
Inwoners, verzekerden, klanten	Laagdrempelige en veilige toegang tot persoonsgebonden diensten	Hoog
Klant Contactcentra VGZ, gemeenten Arnhem en Nijmegen	Afhandelen telefoongesprekken, direct belanghebbend	Hoog
Wijkteams Arnhem en Nijmegen	Toeleiding naar zorg, indirect belanghebbend	Gemiddeld
Backoffice WMO / Participatiewet	Afhandelen complexere vragen, direct belanghebbend	Hoog
CISO	Verantwoordelijke voor compliance binnen de organisatie	Gemiddeld
Privacy officer	Verantwoordelijk voor het juist omgaan met persoonsgegevens binnen de organisatie	Hoog
Wethouder Zorg	Verantwoordelijke voor de dienstverlening op het gebied van de WMO en de Jeugdwet	Gemiddeld
Wethouder Inkomen en armoedebestrijding	Verantwoordelijke voor de dienstverlening op het gebied van de participatiewet	Gemiddeld

2.4 Bestaande voorzieningen

Binnen organisaties wordt dit opgevangen door interne protocollen met 'geheime vragen', dit is echter onmogelijk te realiseren bij telefonische contacten met inwoners. Er zijn echter twee technische oplossingen beschikbaar. Deze voldoen echter ook niet aan de gestelde eisen:

Authenticators

Het is in theorie mogelijk om middels een generieke authenticator van Microsoft, Apple of Google een oplossing te maken voor telefonische authenticatie. Zij hebben echter geen tot op het hoogste niveau vastgestelde persoonsgegevens van een inwoner. De vraag is daarbij ook of het wenselijk is of een dergelijke partij deze persoonsgegevens heeft.

Een andere optie met authenticators is om een 'eigen' app te gebruiken om dit mogelijk te maken. Nadeel hiervan is dat iedere instelling een eigen authenticatieapp moet maken en de inwoner met een groot scala aan apps op de telefoon zit.

Spraakherkenning

Er zijn partijen die werken aan spraakherkenning. Voor identificatie is dit geen haalbare kaart, aangezien telefonie werkt met een 8-bits frequentie. Op deze frequentie, maar ook op het hogere 'digitale' 16bits, is het eenvoudig om spraak te manipuleren door een stem te dupliceren met zowel professionele als publiek toegankelijke software. Tevens zal middels deze oplossing een centrale databank met stemmen moeten worden aangelegd. De vraag is hoe haalbaar én wenselijk dit is.

Binnen dit project wordt gewerkt met de IRMA, deze methodiek is gebaseerd op het Idemix, een cryptografische standaard ontwikkeld door IBM, verrijkt en verder onderbouwd met wetenschappelijke studies door de Radboud Universiteit.

NORA

De gezochte oplossing past tevens binnen de basisprincipes van de NORA:

1. Proactief: De nadruk ligt op het gebruiksgemak. Hoe krijgen we het voor elkaar dat de identificatie aan de telefoon zo vanzelfsprekend is dat iedereen het begrijpt en kan gebruiken.
2. Vindbaar: De authenticatietool moet vanzelfsprekend worden, De data in de tool (vanuit de BRP) eenvoudig en op hoogwaardige kwaliteit te benaderen, en zichtbaar in gebruik
3. Toegankelijk: Door telefonische authenticatie mogelijk te maken, worden persoonlijke diensten voor een grotere doelgroep toegankelijk.
4. Standaard: Hierbij gaan we uit van open standaarden. De ontwikkelde tools zullen open source beschikbaar worden en er wordt gebruik gemaakt van de eIDAS standaarden.
5. Gebundeld: Door deze vorm van authenticatie aan te bieden is het mogelijk om meer diensten telefonisch aan te bieden.
6. Transparant: Het IRMA ecosysteem heeft transparantie als uitgangspunt.
7. Noodzakelijk: Om persoonlijke telefonische diensten aan te kunnen aanbieden is het een deugdelijke identiteitsvaststelling noodzakelijk.
8. Vertrouwelijk: Door de encryptietechniek worden de gegevens alleen doorgegeven aan de persoon die de gegevens mag ontvangen.
9. Betrouwbaar: De inwoner zou er op moeten kunnen rekenen dat de gemeente op een betrouwbare weg, langs alle kanalen, diensten aanbiedt. Dat is momenteel telefonisch niet mogelijk.
10. Ontvankelijk: Door telefonische authenticatie mogelijk te maken wordt een organisatie nog ontvankelijker voor de inwoner.

Daarnaast dient de toepassing te voldoen aan de Digitoegankelijk standaarden EN 301 549 met WCAG 2.1.

Conform de doelstelling van de stichting Privacy by Design, de beheerder van IRMA, wordt alle ontwikkelde software *Open Source* beschikbaar gesteld.

2.5 Projectmanagement

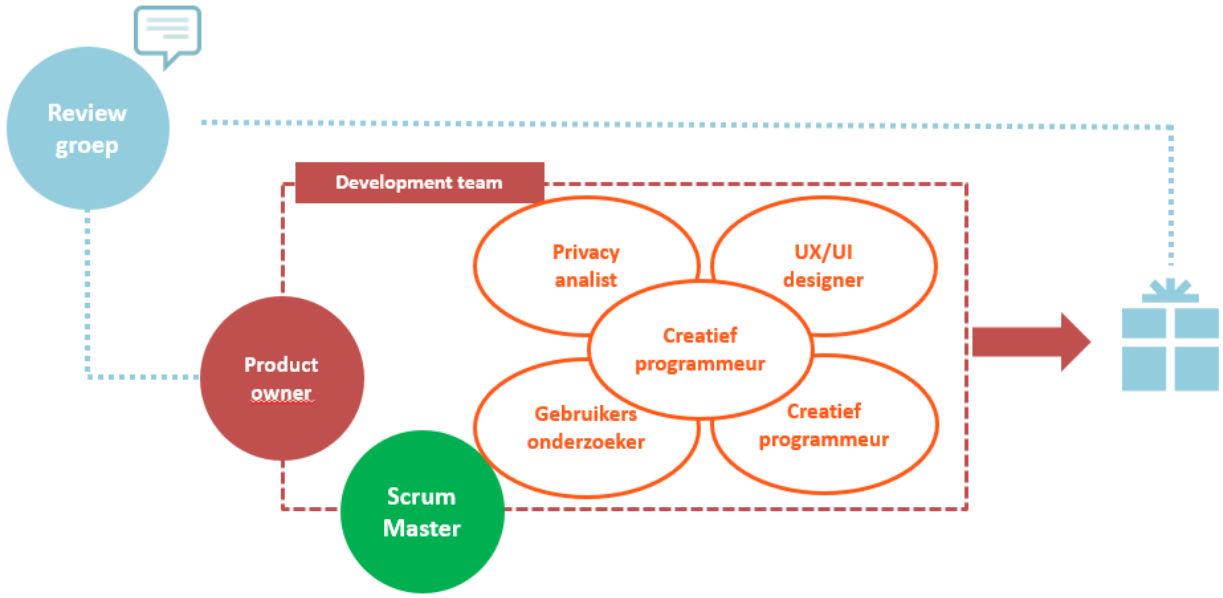
Het project wordt uitgevoerd op basis van de Agile methodiek.

Het developmentteam zal bestaan uit:
- 1 Scrum Master
- 1 Security, privacy en data specialist / analist
- 1 UX/UI designer
- 1 Gebruikersonderzoeker
- 2 Creatief programmeurs

Een productowner / projectleider zal zorgen voor de goede opdrachtformulering en een reviewgroep met minimaal 6 experts zal de opgeleverde producten beoordelen.

Na iedere sprint zal de reviewgroep de voortgang beoordelen en kan waar nodig het sprintdoel voor de volgende sprint aanpassen.

Schematisch ziet dit er als volgt uit:



Een globale planning van de werkzaamheden is als volgt:

Sprint	Datum	Doel
1	30 sep – 11 okt	Onderzoek mogelijkheden
2	14 okt – 25 okt	Prototyping 3 scenario's
3	28 okt – 8 nov	Klanttesten 3 scenario's
4	11 nov – 22 nov	Minimal value product 1 scenario
5	25 nov – 6 dec	Klanttesten scenario
6	9 dec – 20 dec	Proof of concept scenario

2.6 Kosten

De kosten bestaan uit de personeelskosten van de leden van het team. Er zal gewerkt worden met zo veel mogelijk open source tools of, waar nodig, tools vanuit de deelnemende organisaties.

Kosten per sprint:

- Scrum Master	€ 2.808[1]
- een Security, privacy en data specialist / analist	€ 3.168
- een UX/UI designer	€ 2.808
- een Gebruikersonderzoeker	€ 2.808
- Twee Creatief programmeurs	€ 5.616
- Product owner	€ 1.836
- Review team	€ 900
- Totaal	**€19.944**

[1] Verondersteld een sprint van 72 uur, gemiddeld schaal 10, jurist schaal 11 en productowner schaal 12.

De kosten per sprint beslaan ongeveer €20.000, maal 6 sprints is € 120.000.

2.7 Evaluatie en transparantie

Evaluatie

De oplevering van iedere sprint wordt in een reviewsessie geëvalueerd. Iedere 2 weken is er ruimte om het project bij te stellen. De reviewsessies zijn voor iedereen toegankelijk, in ieder geval wordt de expertgroep uitgenodigd.

Aan het eind van het project zal er een grote openbare review worden georganiseerd om het eindresultaat van het project te delen.

Tijdens de evaluaties zal worden gelet op de volgende punten:
- Gebruiksgemak, ook voor personen met een lage digitale vaardigheid
- Functionaliteit, kan een inwoner zich telefonisch authentiseren?
- Veiligheid, welke garanties kunnen worden gegeven over de veiligheid van het systeem?
- Juridisch, voldoet de geboden oplossing aan de wettelijke eisen?
- Toepasbaarheid, kan de oplossing ook toegepast worden bij de opdracht gevende organisaties?

Aan het einde van het proces zal ook een conceptuele penetratietest worden uitgevoerd op de gemaakte oplossing.

Kennisdeling

De oplossing zal gedeeld worden in de landelijke gremia van de opdracht gevende instellingen.

Voor de gemeenten zijn dit in ieder geval:
- VNG realisatie / GGU fonds
- IMG 100.000+
- VIAG
- NVVB

Daarnaast zal er gepubliceerd worden in de vakbladen Burgerzaken en Recht, Digitaal bestuur en Ibestuur.

De HAN Informatica en Communicatie Academie en de gezamenlijke lectoraten van het onderzoekscentrum IT &Media zullen zorgdragen dat de ontwikkelingen rondom 'privacy by design' voor alle digitale kanalen geïntegreerd worden in het onderwijsprogramma voor toekomstige en huidige professionals/ontwerpers/ontwikkelaars in de IT en digitale dienstverlening (media). Daarbij wordt specifiek aangesloten bij de ICT-specialisatie Infrastructure & Security Management, die ook aangeboden wordt als post-HBO-opleiding voor Digital Security Professional. De partijen zullen optreden als opdrachtgever voor studentenprojecten. We kijken naar de mogelijkheden om studenten mee te laten werken (als stage) in de sprints.

Radboud University zal het project versterken met expertise op het gebied security en privacy. Het onderzoek naar telefonische identificatie zal worden ingebed in iHub (Interdisciplinary Hub for Security, Privacy and Data Governance). De rol van iHub richt zich in het bijzonder op de evaluatie van het system ten opzichte van functionaliteit en veiligheid.

Openheid en transparantie

De gemaakte software zal worden gepubliceerd als open source code. Daarnaast is het hele traject open en transparant. Alle reviews zullen openbaar toegankelijk zijn en de finale oplevering aan het einde van sprint 6 zal worden aangekondigd.

2.8 Toekomstplan

Het toekomstplan is afhankelijk van het resultaat vanuit dit project. Hieronder worden een aantal

scenario's geschetst:

Project levert een werkende oplossing op
Indien het project een werkende oplossing oplevert, zal deze worden uitgerold bij de betrokken organisaties. Allereerst in pilotvorm op kleine schaal, bij goed resultaat op grotere schaal binnen de betrokken organisaties en vervolgens binnen andere organisaties.

Project levert een bruikbare Proof of Concept op
Indien het project een Proof of Concept oplevert, zal het project voortgezet worden via dezelfde methodiek om de Proof of Concept door te ontwikkelen tot een werkende oplossing.

Project levert een bruikbaar concept op
Indien het project een bruikbaar concept oplevert, zal het project worden voortgezet met personen of partijen die het bruikbare concept kunnen omzetten naar een Proof of Concept.

Verantwoordelijkheid en kosten
De betrokken partijen hebben belang bij een oplossing en hebben zich verenigd in het netwerk SlimID, dat gericht is op kennisdeling en versterking rondom digitale identiteitsoplossingen, vanuit het perspectief van human-centered design and engineering. Dit consortium zal de verantwoordelijkheid nemen om dit probleem op te lossen, mits er een werkende oplossing in het verschiet ligt.

Het consortium bestaat uit bedrijven en instellingen uit verschillende sectoren (overheid, zorg, onderwijs, software). Via de diverse subsidiemogelijkheden zal gekeken worden naar financiering voor

2.9 Risico's

Risico	**Kans**	**Impact**	**Kans * Impact**	**Aanpak**
Geen developers beschikbaar	9	2	18	Minder werkend product maken (MvP)
Complexiteit van het onderwerp is te groot	8	8	64	Werken in korte sprints

2.10 Contactgegevens samenwerkingspartners

Deze oplossing wordt ingediend door twee gemeenten, twee kennisinstellingen, een zorgverzekeraar en een leverancier van ICT-oplossingen in de zorg. In onderstaande tabel staan de contactpersonen van de betrokken partijen.

Organisatie	**Contactpersoon**	**e-mail**
Gemeente Nijmegen	[redacted]	[redacted]
Gemeente Arnhem	[redacted]	[redacted]
Hogeschool Arnhem Nijmegen	[redacted]	[redacted]
Radboud Universiteit	[redacted]	[redacted]

Coöperatie VGZ UA	[redacted]	[redacted]
Vtel telecom	[redacted]	[redacted]