Voorstel

Technisch partnerschap ID-contact

Naar aanleiding van de offerte uitvraag ID-contact, voor het consortium onder leiding van:

GEMEENTE Arnhem

[redacted]

3 september 2020

tweede golf
wij zijn web engineers

INLEIDING

In de periode januari 2020 t/m april 2020 heeft Tweede golf met veel plezier en enthousiasme de rol van technisch partner vervuld in het ID-bellen / Veilig bellen project, voor de gemeenten Arnhem, Nijmegen en Drechtsteden. Nu er zal worden doorontwikkeld op basis van het proof-of-concept dat in dit project gerealiseerd is, is Tweede golf uiteraard enthousiast ook voor die doorontwikkeling de rol van technisch partner op zich te nemen.

Met deze offerte bieden we het consortium onder leiding van de gemeente Arnhem aan om - op vergelijkbare wijze als bij Veilig bellen - een compact development team van Tweede golf in te huren dat de ontwikkeling van alle benodigde software op zich zal nemen, in nauwe samenwerking met de product owner die door de opdrachtgever zal worden aangesteld en andere partijen zoals bijvoorbeeld PbDF[1].

Hieronder gaan we eerst nader in op onze motivatie en - naar ons oordeel - onze geschiktheid om bovengenoemde rol te vervullen. Achtereenvolgens komen aan bod:

[1] De Privacy by Design Foundation, voorgezeten door Bart Jacobs, hoogleraar computerbeveiliging aan de Radboud Universiteit te Nijmegen.

MOTIVATIE EN GESCHIKTHEID

Technisch partnerschap in het ID-contact project zien wij als een rol die ons op het lijf geschreven is. Bovendien zien wij het als een uitgelezen kans om de kennis die is opgedaan binnen het project Veilig bellen (maar ook binnen Veilig Jitsi en IRMA Balie, zie verderop) in te zetten om een serieuze bijdrage te leveren aan een volgende stap op weg naar moderne privacyvriendelijke (digitale) dienstverlening, door ontwikkeling van wat in de uitvraag omschreven wordt als ‘een authenticatiemethode die inclusief en omnichannel is [en] die door zowel de overheid als private partijen te gebruiken is’.

Het doel van dit project en de setting passen bovendien goed bij wat we met Tweede golf beogen te doen: software ontwikkelen die ertoe doet, in nauwe samenwerking met de opdrachtgever en anderen en binnen domeinen waar we daadwerkelijk iets voor voelen en kundig zijn.

Hieronder noemen we een aantal zaken die naar onze mening onze geschiktheid voor de rol van technisch partner onderstrepen.

BETROKKENHEID BIJ PBDF EN IRMA

Sinds begin dit jaar draaien we mee in de SLA voor de ‘IRMA backbone’ die PbDF aan SIDN levert en is een goede samenwerking ontstaan met het team van PbdF onder leiding van [redacted]

Sinds deze zomer mogen we onszelf met trots *preferred partner* noemen van PbDF, wat zoveel betekent dat we de partij van eerste keuze zijn voor PbDF als het gaat om IRMA gerelateerde implementaties, zie de vermelding op https://privacybydesign.foundation/gebruik/.

Naast onze rol als technische partner voor het Veilig bellen project, zijn we ook betrokken geweest bij de ontwikkeling van de IRMA app voor de gemeente Amsterdam, bij een experiment met het gebruik van IRMA met Jitsi (gemeente Nijmegen) en zijn we momenteel bezig met een nieuw, veelbelovend op IRMA-gebaseerd project voor de gemeente Amsterdam genaamd IRMA Balie.

PRIVACY & SECURITY EXPERTISE

Binnen Tweede golf is al jaren security kennis aanwezig bij mensen als [redacted]. In het bijzonder behaalde [redacted] security audits uitgevoerd op onder andere overheidsprojecten, vanuit het Laboratory for Quality Software[2].

[2] Zie https://www.ru.nl/icis/valorization/laboratory-quality/

Daarnaast is privacy sinds de introductie van de AVG een actueel thema binnen Tweede golf dat serieus genomen wordt en waar frequent aandacht voor is.

Tenslotte: door deelname aan eerder genoemde IRMA-gerelateerde projecten is specifieke kennis aanwezig met betrekking tot hoe binnen IRMA en binnen gemeentes met privacy en security gerelateerde zaken wordt omgegegaan en zijn er inmiddels vijf ontwikkelaars van Tweede golf ingewerkt in IRMA.

ERVARING MET PRODUCTONTWIKKELING EN ONDERZOEK

Tweede golf heeft inmiddels meer dan 10 jaar ervaring met de ontwikkeling van digitale producten en diensten, waarbij agile wordt gewerkt en de laatste jaren steeds meer gebruik wordt gemaakt van de lessen van Lean startup[3]. We zijn hier zeer enthousiast over en we denken dat onze ervaring hiermee goed past bij de onderzoeksinslag van het ID-contact traject: samen, al onderzoekend, iteratief de best mogelijke oplossingen realiseren.

Daarnaast hebben alle ontwikkelaars vanuit hun studieachtergrond (meestal WO) ervaring met onderzoek en doen we binnen Tweede golf continu onderzoek naar opkomende technologieën.

HART VOOR OPEN SOURCE

Bij Tweede golf hebben we hart voor open source en werken we met een moderne stack bestaande uit open source technieken, waaronder Node.js, React, Rust en Go[4]. Een selectie van onze open source bijdragen (o.a. irma-jitsi) staat hier: https://tweedegolf.nl/open-source.

Het doet ons dan ook goed dat de source code die in het kader van ID-contact geproduceerd zal worden gepubliceerd wordt onder de EUPL-1.2 licentie[5].

Zie https://github.com/tweedegolf voor een volledig overzicht van wat we tot nu toe, ook met betrekking tot IRMA, geopensourced hebben.

Naast dat we actief open-source projecten onderhouden, participeren we ook bij verschillende open-source projecten door in dialoog te treden bij issues en pull requests in te dienen. In het bijzonder hebben we ook contributies gedaan aan het IRMA project zelf en aan het Jitsi videoconferencing project.

---

[3] Zie https://en.wikipedia.org/wiki/Lean_startup. Lean startup is er samenvattend op gericht om zo snel mogelijk en zo 'goedkoop' mogelijk te valideren of een beoogde oplossing ook daadwerkelijk werkt voor de beoogde gebruikers.

[4] Dit zijn voorbeelden van technieken/talen die wij prefereren en waarmee we productiewaardige software bouwen. Alle ontwikkelaars van Tweede golf zijn in meerdere talen thuis, ook andere dan de genoemde.

[5] We gaan ervan uit dat opdrachtgever zorg zal dragen voor het beheer van de open source projecten die zo ontstaan en indien nodig in overleg Tweede golf inschakelt voor onderhoud of doorontwikkeling.

Deze houding ten opzichte van open source betekent ook dat het in projecten onze voorkeur heeft om open source oplossingen en open standaarden te gebruiken voor zover dat mogelijk is, zowel uit kostenoverweging als met het oog op doorgaand onderhoud van de software. Echter, het kan voorkomen dat dit voor sommige onderdelen niet of moeilijk haalbaar is. Een voorbeeld (uit Veilig bellen) is het integreren met een telefooncentrale: eindgebruikers zullen al snel de voorkeur geven voor een low-effort in de cloud gebaseerde oplossing. In zo'n geval zullen wij realistische oplossingsrichtingen adviseren.

OVERIGE RELEVANTE ERVARING

In de offerte uitvraag wordt ook gevraagd naar ervaring met betrekking tot CI/CD en testen, het ontwerpen en realiseren van veilige code en ervaring binnen het publieke domein. Hieronder gaan we daar nader op in.

Ervaring met CI/CD en testing

Alle projecten binnen Tweede golf worden reeds met een volwassen Continuous Integration workflow volgens industriestandaarden ontwikkeld. Concreet wil dit zeggen dat alle code-producten gedurende de ontwikkeling per feature (in een zgn. feature branche) naar een centrale code repository gestuurd worden. Afhankelijk van de eisen van het project worden in de software ontwikkelstraat ook automatische tests gedraaid en eventueel wordt het eindproduct op een testomgeving gedeployed.

Voor codebeheer gebruiken we doorgaans 'git' in een self-hosted GitLab-omgeving. De software ontwikkelstraat wordt verzorgd door zowel lokale servers in het kantoor van Tweede golf als externe servers in de cloud. Online backend systemen worden gedeployed op virtual machines (door middel van Ansible) en/of Kubernetes bij verschillende cloud vendors, waaronder Amazon, TransIP en Google.

De opzet van de software ontwikkelstraat en bijbehorende werkwijze worden per project bepaald, afhankelijk van de specifieke eisen van het project en de best practices die we binnen Tweede golf hanteren. Voor het Veilig Bellen project bijvoorbeeld vindt de ontwikkeling plaats op Github, met een Travis CI ontwikkelstraat. Als ervaren DevOps en SysOps team zijn we hierin flexibel.

Kennis en ervaring m.b.t. ontwerpen en realiseren veilige code

Bij Tweede golf zijn we ervan overtuigd dat veilige code en systemen alleen kunnen voortkomen uit een veilig proces. Hiervoor hanteren we een set best practices, die op maat voor elk project aangepast worden. Zo bestaat er doorgaans voor proof-of-concepts noch de behoefte, noch het

budget om alle best practices aan te houden; terwijl voor een MedTech gerelateerd project strikte kwaliteitseisen gelden[6].

Dat gezegd hebbende bestaat ons inziens in zijn algemeenheid een verantwoord ontwikkelproces uit de volgende elementen:

- Een veilige architectuur als basis met een goed gedefinieerd security- en threat-model.
- Het gebruik van de geschikte middelen, zoals inherent veilige talen (zoals Go of Rust) en volwassen libraries.
- Consequent toepassen van code reviews volgens het four-eyes-principe.
- Een pre-compliance security audit door het ontwikkelteam.
- Een post-development security audit door een onafhankelijk bureau.
- Een post-development lifecycle process voor zowel software als systeembeheer, met in het bijzonder ruimte voor software updates van dependencies.

Binnen Tweede golf beschikken we zowel over relevante praktijk- als academische-kennis op het gebied van security architectuur, het beheren van Software of Unknown Pedigree[7] en dependency management, het werken met code review procedures, het uitvoeren van interne en externe security audits en penetration tests, en het onderhoud van projecten die in productie worden gebruikt maar die niet actief worden doorontwikkeld.

Telefoniecentrales

Vanuit Tweede golf hebben we praktijkervaring met de open source telefoniecentrale Asterisk, alsmede de cloud-based telefoniecentrales Amazon Connect en Twilio.

Ervaring binnen het publieke domein

Naast genoemde IRMA projecten voor de gemeenten Nijmegen en [redacted] heeft Tweede golf in het verleden ook:

- [redacted]

Vanuit deze projecten hebben we bijvoorbeeld ook ervaring met samenwerking met externe partijen die onze implementatie van de web toegankelijkheidsrichtlijnen toetsen.

[6] Het afgelopen jaar heeft het team dat aan Veilig bellen werkte binnen Tweede golf ook aan een MedTech project gewerkt, te weten de ontwikkeling van firmware voor de nieuwe holter-ecg van Glanum Medical, waarbij strikte kwaliteitseisen zijn gehanteerd en het team onder andere processen heeft geimplementeerd en documentatie heeft opgeleverd volgens de IEC 62304 standaard voor de ontwikkeling van medische software.

[7] Ook wel SOUP genoemd, zie https://en.wikipedia.org/wiki/Software_of_unknown_pedigree.

Testimonials
Tot slot verwijzen we naar Bijlage 1 Testimonials om twee van onze opdrachtgevers aan het woord te laten.

INVULLING EN WERKWIJZE

Zoals reeds in de inleiding genoemd stellen we als concrete invulling van het technisch partnerschap voor dat Tweede golf gedurende de looptijd van het project een compact development team[8] levert dat onderdeel zal uitmaken van het ID-contact projectteam[9].

Het development team zal van A tot Z zorgdragen voor de ontwikkeling van alle benodigde technische componenten, onder aanvoering staan van een product owner aangewezen door de opdrachtgever en nauw samenwerken met de andere leden van het projectteam en indien nodig bijvoorbeeld met de ontwikkelaars van PbDF.

SCRUM ALS BASIS

In de offerte uitvraag wordt gesproken over 6 sprints, van ieder een maand in de periode oktober 2020 t/m april 2021[10] en aansturing van het development team (en projectteam) door één overkoepelende product owner. In het bijzonder wordt nog grotendeels open gelaten hoe de deliverables er precies uitzien. Deze agile aanpak, die gebaseerd is op het vertrouwen naar elkaar om binnen de bestaande constraints van doorlooptijd en budget zoveel mogelijk waarde te creëren - en die veel lijkt op de aanpak die we voor Veilig bellen hanteerden - juichen we van harte toe.

Net als in ons voorstel voor Veilig bellen benadrukken we dat het voor ons veel belangrijker is om de principes waar scrum op is gebaseerd als uitgangspunten voor een succesvolle samenwerking te hanteren dan de scrum guide[11] tot op de letter te volgen. In onze projecten willen we altijd terugzien:

- Een duidelijke rolverdeling (product owner, developers, stakeholders), met in het bijzonder een sterke product owner rol.
- Inspect & adapt: frequente, periodieke inspectie van zowel het product (Wat hebben we tot nu toe?) als het proces (Werken we optimaal met elkaar?).

[8] Zie voor de samenstelling verderop onder Samenstelling development team.

[9] Het team waarin ook [redacted] zullen zitten voor gebruikersonderzoek en [redacted].

[10] In de maanden december en januari wordt 1 sprint gedaan.

[11] Zie https://www.scrum.org/resources/scrum-guide.

- Continuïteit en structuur: werken op vaste dagen in de week, met vaste momenten om te plannen en te inspecteren.
- Gezamenlijkheid: samen het product en proces inspecteren, samen plannen, etcetera, zodat er steeds een *common understanding* is van wat er moet gebeuren en waarom.

De precieze werkwijze - op basis van deze uitgangspunten - bepalen development team en product owner bij aanvang in overleg. Degene die de scrum master rol vervult (zie Samenstelling development team) zal hier in overleg met de product owner het voortouw in nemen.

WERKRITME

We stellen in de basis voor om - in lijn met bovenstaande uitgangspunten - de beschikbare capaciteit zoveel mogelijk gelijk te verdelen over de 6 sprints en in overleg 2 vaste dagen in de week te kiezen waarop het development team de werkzaamheden zal uitvoeren. Zie verder onder Budget en planning.

LOCATIE

Tweede golf is gevestigd in de Nijmeegse wijk Bottendaal op ongeveer 10 minuten fietsen van zowel het gemeentehuis als de universiteitscampus. Het development team voert de ontwikkelwerkzaamheden uit op locatie bij Tweede golf[12]. Het team heeft daar met de product owner de beschikking over de zgn. '*project room*', een ruimte die erop is ingericht als (scrum) team effectief samen te werken.

De product owner is zoveel als nodig aanwezig bij Tweede golf om face to face met zijn team samen te werken. Afhankelijk van de fase waarin de softwareontwikkeling zich bevindt (en het aantal dagen dat het team werkt) is dit bijvoorbeeld één dag per week.

HOSTING

We verzorgen voor onze klanten standaard de hosting en operations van ontwikkelde applicaties.

We zijn ervaren op het gebied van hosting en operations voor zowel 'bare-metal' op linux gebaseerde omgevingen, als virtuele containers gebaseerd op Docker in Kubernetes. Per applicatie zal in overleg een geschikte omgeving worden gekozen[13].

[12] Voor zover de regels met betrekking tot corona en de wensen van de opdrachtgever hieromtrent dit toelaten.
[13] Voor videoconferencing-platforms zoals Jitsi, of telefooncentrales zoals Asterisk geldt bijvoorbeeld dat het doorgaans efficiënter is om direct op 'bare-metal te draaien'.

De afspraken omtrent hosting en bijbehorende dienstverlening (eventueel een SLA) zullen ter zijner tijd in een separate overeenkomst worden vastgelegd.

SAMENSTELLING DEVELOPMENT TEAM

WOB art.10 2 g

We stellen voor om het team dat aan Veilig bellen heeft gewerkt opnieuw als kernteam in te zetten. Dit team bestaat uit de volgende personen:

[redacted]

MOTIVATIE

Bij Tweede golf kijken we altijd naar de meest geschikte teamsamenstelling gegeven de opdracht die voorligt. We kijken daarbij in eerste instantie naar zaken als relevante inhoudelijke kennis en ervaring, ervaring met werken met elkaar en ervaring met de context. Voor bovenstaand team geldt dat al deze zaken naar ons oordeel in ruim voldoende mate aanwezig zijn. Naast bij Veilig bellen, heeft bovengenoemd team bijvoorbeeld ook gewerkt aan eerder genoemde firmware voor de nieuwe holter-ecg van Glanum Medical.

Ten tweede stellen we als eis dat de ‘tech lead rol’ en ‘project lead rol’ goed kunnen worden ingevuld.

TECH LEAD EN PROJECT LEAD

De tech lead is degene die eindverantwoordelijk is voor alle techniek en bijvoorbeeld uiteindelijk de knopen doorhakt waar het gaat om architectuurkeuzes.

De project lead is degene die de rol van scrum master vervult[14] en daarnaast zorgt dat organisatorische zaken zoals planning en reporting in orde zijn.

[14] In de praktijk: zorgen dat ‘alles soepel loopt’, dat de uitgangspunten die het team zelf heeft gekozen goed worden toegepast en dat de product owner begeleid wordt in zijn rol indien nodig.

PERSOONLIJKE KENNIS EN ERVARING

[redacted]

CONTINUÏTEIT VAN DE TEAMSAMENSTELLING

Uitgangspunt is wat Tweede golf betreft dat de teamsamenstelling gedurende de hele looptijd constant blijft maar dat er ruimte is om, mocht zich een uitzonderlijke situatie voordoen, in overleg met opdrachtgever één van de teamleden te wisselen. Mocht dat betekenen dat een andere ontwikkelaar van Tweede golf moet worden ingewerkt, dan doet Tweede golf daarvoor vooraf een eigen investering zodat het team niet aan *velocity* verliest.

ONDERSTEUNING VANUIT MT

Alhoewel het team samen met de product owner als zelforganiserend team zal opereren staat het er niet alleen voor. Binnen Tweede golf [redacted] zal periodiek meekijken met en als klankbord fungeren voor de technische keuzes die gemaakt worden. Op eenzelfde manier zal [redacted] periodiek als klankbord fungeren voor keuzes die gemaakt worden met betrekking tot planning en proces.

OVERIGE ONDERSTEUNING

Mocht er specialistisch frontend-werk verricht moeten worden, dan kan [redacted] team incidenteel ondersteunen. [redacted] Tweede golf heeft onder andere

voor bovengenoemde projecten binnen het publieke domein deze richtlijnen meerdere keren en op verschillende niveau's geimplementeerd.

Mocht er voor een onderdeel specifieke UX en/of design expertise nodig blijken te zijn, dan kan indien gewenst laagdrempelig worden samengewerkt met [redacted][15] Tweede golf staat echter ook open voor samenwerking met een andere partij op dit vlak.

BUDGET EN PLANNING

BUDGET

In de offerte uitvraag zijn doorlooptijd [redacted] gegeven.

[redacted]

PLANNING

Zoals reeds opgemerkt onder Werkritme stellen we voor de beschikbare capaciteit zoveel mogelijk gelijk te verdelen over de 6 sprints, waarbij iedere sprint in principe één kalendermaand duurt en waarbij steeds op vaste dagen in de week door het development team (en de product owner) wordt gewerkt.

[redacted] Dit heeft als voordeel dat we:

- enige flexibiliteit behouden mocht blijken dat in de eindfase nog extra afrondende werkzaamheden nodig zijn en
- dat het mogelijk is in overleg tijdelijk iets meer dan de gemiddelde capaciteit in te zetten, bijvoorbeeld wanneer er een sprint in de planning staat waarvan verwacht wordt dat die een meer dan gemiddelde effort zal vergen.

---

15 [redacted]

16 [redacted]

[redacted] Precieze startdatum in overleg.

[redacted]

RESERVERING CAPACITEIT

Omdat Tweede golf de benodigde capaciteit ver vooruit reserveert, gaan we ervan uit dat ten minste ⅔ daarvan ook daadwerkelijk wordt afgenomen en dat de product owner er zorg voor draagt dat het development team te alle tijden vooruit kan.

FACTURATIE

De facturatie geschiedt maandelijks achteraf voor de gemaakte uren.

VOORWAARDEN EN ACCORDERING

Indien opdrachtgever akkoord geeft op deze offerte zullen opdrachtgever en Tweede golf een separate overeenkomst opstellen voor de levering van de in deze offerte omschreven dienstverlening. Op die overeenkomst zullen de GIBIT voorwaarden (versie 2016) van toepassing zijn. In overleg zullen enkele uitzonderingen worden gemaakt op bepalingen die niet goed passen bij de beoogde agile manier van werken en gedeelde budgetverantwoordelijkheid.

[redacted]

[redacted]

[redacted]

BIJLAGE 1 TESTIMONIALS

[redacted]