Tijdelijke opdracht: Aanvraag Dienst Pentest DigiD (opdrachtnummer:3.24)

Graag nodigen wij u uit om een offerte uit te brengen voor de dienst van een pentest voor een nieuwe DigiD aansluiting. De formulierenomgeving wordt door de leverancier gemigreerd van versie 4.2 naar versie 4.3. Bij deze migratie wordt een nieuwe DigiD aansluiting geïnstalleerd met een SAML koppelvlak i.p.v. het CGI koppelvlak bij de gemeente Stichtse Vecht. De gemeente Stichtse Vecht beoogt een Nadere Overeenkomst af te sluiten op basis van de Raamovereenkomst GGI veilig – "Security Expertisediensten" perceel 3.

We richten ons in deze uitnodiging uitsluitend tot gecontracteerde Opdrachtnemers van GGI veilig "Security Expertisediensten" perceel 3.

Op deze offerteaanvraag is de Raamovereenkomst GGI veilig "Expertise diensten" (Perceel 3) en alle bijbehorende documentatie van toepassing, die als bijlage bij de offerteaanvraag beschikbaar is gesteld op CTM Solution. Verder zijn de ARVODI-2018 voorwaarden van toepassing. Eventuele afwijkingen op ARVODI-2018 worden benoemd in de raamovereenkomst.

De gepubliceerde offerteaanvraag op CTM Solution met aanbestedingsnummer 248311 is leidend boven elders gepubliceerde documenten. De eisen en wensen zijn bij eventuele discrepanties leidend boven het gestelde in de profieltekst.

Specifieke gegevens aanvraag Dienst	
Expertise gebied	Keuze uit: ☐ SIEM proces ☐ Compliancy ☐ Vulnerability ☒ Pentesten ☐ Forensics* ☐ Hardening ICT Infrastructuur
Plaats tewerkstelling	Het Gemeentehuis in Stichtse Vecht of vanuit eigen locatie. Dit is nader te bepalen.
Gewenste startdatum	Circa 21-10-2020
Tussentijdse oplevertermijnen (optioneel)	Datum: Resultaat:
Einddatum	Circa 28-10-2020 rapportage zsm aanleveren na testen.
Contractvorm	☒ Vaste prijs

	☐ Nacalculatie (met plafond)
Spoedprocedure	☐ Ja (alleen in geval van Forensics) ☒ Nee
*Gebruik uitkomst onderzoek voor strafrechtelijke vervolging	☐ Ja, de uitkomst van het forensisch onderzoek wordt voor strafrechtelijke vervolging gebruikt ☐ Nee, uitkomst wordt niet strafrechtelijk gebruikt (let op: Indien Ja, uitkomst wordt gebruikt voor strafrechtelijke vervolging, zijn speciale opleidingen en accreditaties benodigd. Deze dienen te worden ingevuld bij 2. Eisen)

Voorgenomen planning	
Verzending offerteaanvraag	3 september 2020
Uiterste datum stellen vragen	8 september 2020, 12:00 uur
Uiterste verzenddatum beantwoorden vragen	10 september 2020
Uiterste datum indienen offertes	24 september 2020, 12:00 uur
Beoordeling van offertes en voorgenomen gunning	1 oktober 2020
Opschortende termijn	1 oktober 2020
Definitieve gunning	9 oktober 2020

1. Specificatie

1.1 Over Stichtse Vecht

Stichtse Vecht is een gemeente in de provincie Utrecht en ligt tussen de steden Utrecht, Hilversum en Amsterdam. Centraal door de gemeente loopt de rivier de Vecht. De gemeente is op 1 januari 2011 ontstaan door samenvoeging van de gemeenten Breukelen, Loenen en Maarssen. Stichtse Vecht heeft ruim 64000 inwoners en het gemeentehuis is in Maarssen.

1.2 Over het Online Team

Het Online Team valt organisatorisch onder team Bestuurs- en directieondersteuning en onderhoud het intranet, de websites stichtsevecht.nl en trouweninstichtsevecht.nl, webformulieren en de daarbij behorende diensten, zoals DigiD.

1.3 Omschrijving van de gevraagde dienst

Alle organisaties die gebruik maken van DigiD moeten voldoen aan de beveiligingsnorm v2.0. Deze norm is gebaseerd op de ICT beveiligingsrichtlijnen voor webapplicaties van het NCSC. Via een ICT beveiligingsassessment moet dit worden getest. Een pentest is onderdeel van dit assessment. Wij moeten de pentest laten uitvoeren voor een nieuwe DigiD aansluiting met een SAML koppelvlak i.p.v. CGI koppelvlak. Voor de DigiD pentest is een blackbox/greybox benadering, waarbij zonder veel voorkennis ingelogd wordt als gebruiker, voldoende.

In de offerte ook een hertest meenemen van de bevindingen, nadat ze zijn opgelost.

De formulieromgeving van Stichtse Vecht draait op een externe server, in een saas-omgeving. Er is een OTAP-straat. Bij ongeveer 50 van de ongeveer 70 formulieren wordt DigiD gebruikt, bij een aantal formulieren reken je gelijk online af en bij een enkel formulier wordt gebruik gemaakt van eHerkenning. De formulieren staan gebundeld op https://stichtsevecht.nl/online-regelen-overzicht-formulieren/

Voorbeelden:

- Formulier met DigiD en online afrekenen: Uittreksel persoonsgegevens
- Formulier zonder DigiD en online afrekenen: Tuinzak

De scope van de toetsing is de internet-facing webpagina, de formulieren, systeemkoppelingen en infrastructuur die met DigiD gekoppeld zijn en betrekking hebben op het proces.

1.4 Resultaat van de gevraagde dienst

1.4.1 Beoogde resultaat

De gemeente moet aantoonbaar voldoen aan de door Logius gestelde ICT Beveiligingsrichtlijnen voor webapplicaties. Alle bevindingen die uit de penetratietest voortkomen dienen vastgelegd te worden.

1.4.2 Resultaat vorm (bijvoorbeeld rapport, presentatie, adviesgesprek)

Het resultaat dient een rapport te zijn en kan in een presentatie worden toegelicht.

De rapportage moet voorzien zijn van:

- Classificatie van de rapportage.
- Beschrijving van de gebruikte technieken.
- Beschrijving object van het onderzoek: webfacing infrastructuur, servers, verbindingen.
- Overzicht afwijkingen ten opzichte van de norm met bijbehorende mate van risico o.b.v. norm.
- Overzicht en details resultaten en afwijkingen per onderdeel uit de norm.
- Proof of Concepts of details in rapportage waarmee de bevinding kan worden gereproduceerd.
- Concrete aanbevelingen per bevinding.

1.4.3 Beschrijving van de vorm van het resultaat

Voor de rapportage wordt gebruik gemaakt van een standaard manier van rapporteren. De presentatie kan plaatsvinden op het gemeentehuis in Maarssen of via Teams. Onze auditor ontvangt ook een rapport van deze pentest. Opdrachtnemer van de pentest moet bereikbaar zijn voor vragen van de auditor. De rapportage moet zo spoedig mogelijk na het testen (binnen 2 werkweken) worden aangeleverd.

Graag een voorbeeld rapportage als bijlage meesturen bij de offerte.

2. Beoordelings- en gunningsprocedure

In dit hoofdstuk zijn achtereenvolgens beschreven: de beoordelingsprocedure, de gunningsprocedure en de mogelijkheden om naar aanleiding van de gunningsbeslissing vragen te stellen of bezwaar in te dienen.

2.1 Beoordelingsprocedure

Er wordt eerst inhoudelijk gecontroleerd of de inschrijvingen voldoen aan de eisen. Inschrijvingen, die niet aan de eisen voldoen, worden niet verder in behandeling genomen. Het ontbreken van informatie of antwoorden, bijvoorbeeld door onjuiste of onvolledige overname van overzichten, gegevens en verklaringen, is voor eigen risico van de opdrachtnemer, en kan leiden tot uitsluiting.

In de eerste plaats worden de aanbiedingen beoordeeld op het voldoen aan de gestelde eisen. Bij twijfel over de juistheid van antwoorden kan telefonisch contact worden opgenomen voor verificatie. Als voor een bepaald aspect uitdrukkelijk bewijs in het plan van aanpak is gevraagd en dat bewijs ontbreekt (in de ogen van de beoordelaar), dan kan zonder verificatie worden besloten de offerte terzijde te leggen.

2.2 Programma van Eisen

Hieronder worden de eisen beschreven die van toepassing zijn op deze opdracht. Voor de wijze waarop deze eisen moeten worden beschreven wordt verwezen naar de invulinstructie.

Programma van Eisen Uit het aangeleverde uitvoeringsvoorstel blijkt minimaal dat de aanbieding van de Opdrachtnemer aantoonbaar beschikt over:
Kandidaat tekent een integriteit en geheimhoudingsverklaring.
Kandidaat levert na gunning een VOG aan die niet ouder is dan 3 jaar en die getoetst is op het type uit te voeren werkzaamheden.
Kandidaat is onderdeel van een team aan pentesters.
Opdrachtnemer zet enkel pentesters in die minimaal voldoen aan het profiel: ▪ In de afgelopen 2 jaar minimaal 4 pentesten zelfstandig uitgevoerd ▪ Minimaal 3 jaar ervaring met het uitvoeren van pentesten ▪ Minimaal 3 jaar ervaring in rapporteren van bevindingen en adviseren van maatregelen ▪ Kennis van professionele tooling (Zoals o.a. OWASP, Metasploit) ▪ Kennis en ervaring met uitvoeren van DigiD pentesten • Communicatie, rapportage en presentatie in de Nederlandse taal

2.3 Kwaliteit

Nadat de inschrijvingen zijn gecontroleerd op de eisen, worden de wensen (lees: kwaliteit) beoordeeld.

De score op de wensen (kwaliteit) telt voor 70% mee.
Kwaliteit wordt voor de uitvraag van een opdracht beoordeeld door middel van een Plan van Aanpak (ook wel uitvoeringsvoorstel genoemd). In het Plan van Aanpak dient de Opdrachtnemer per gekozen onderwerp aan te geven op welke manier zo optimaal mogelijk wordt aangesloten op de door de deelnemer gevraagde dienstverlening.

2.3.1 Onderwerpen Plan van Aanpak

Ieder onderwerp in het Plan van Aanpak heeft een wegingsfactor op basis van relevantie ten behoeve van het bepalen van de totaalscore. De totaalscore moet altijd op 100% eindigen.

Scoretabel voor perceel 3		Maximaal aantal punten	Wegingsfactor	Maximaal A4 per antwoord
1	Beschrijving onderzoeks-/auditaanpak en rapportage	100	20	1
2	Beschrijving technieken en tools	100	15	1
3	Stappenplan met activiteiten in volgorde en doorlooptijd	100	35	3
4	Beschrijving van de beveiligingsrichtlijnen / normen	100	20	1
5	Omschrijving integriteit en screening medewerkers	100	10	1
			Totaal 100%	

Voor de wijze waarop deze wensen kunnen worden beschreven wordt verwezen naar de invulinstructie.

2.3.2 Beoordeling Kwaliteit

Omwille van de objectiviteit worden de kwalitatieve subgunningscriteria beoordeeld op het moment dat de beoordelaars nog geen kennis hebben van de prijzen. Voor de beoordeling van het plan van aanpak wordt een meetinstrument gehanteerd dat gebruik maakt van rapportcijfers. Per onderwerp van het Plan van Aanpak wordt een score toegekend, dit gebeurt door de individuele beoordelaars.

Er wordt beoordeeld conform onderstaande tabel. Onderstaande tabel is uitputtend en zal door alle beoordelaars worden toegepast. Andere rapportcijfers en getallen achter de komma worden niet toegekend door de individuele beoordelaars.

Rapportcijfer	Toelichting
100	Uitstekend, beantwoording voldoet volledig aan het gevraagde, blijk geeft het gevraagde volledig te doorgronden, optimaal bijdraagt aan het gewenste resultaat en adequaat inspeelt op de specifieke situatie van de Deelnemer. De beantwoording is tevens concreet en realistisch.
62,5	Goed, beantwoording voldoet goed aan het gevraagde, sluit goed aan bij de behoeften en wensen van Deelnemer en geeft blijk van goed inzicht in de situatie van de Deelnemer. Beantwoording is concreet en realistisch.
25	Voldoende, beantwoording sluit grotendeels aan bij het gevraagde en sluit redelijk aan bij behoeften en wensen van Deelnemer, of beantwoording is in beperkte mate concreet en/of realistisch.
0	Onvoldoende, beantwoording voldoet onvoldoende aan het gevraagde en/of sluit onvoldoende aan bij behoeften en wensen van aanbestedende dienst, of beantwoording is niet concreet en/of niet realistisch.

Het plan van aanpak wordt door minimaal twee beoordelaars beoordeeld. In een plenair overleg worden de argumenten die hebben geleid tot de individuele punten besproken. Daarna komt het beoordelingsteam in consensus tot een unaniem oordeel inclusief motivatie.

4. Prijs

Inschrijvers dienen het bijgevoegde Prijzenformulier (bijlage 2) volledig in te vullen en op het aanbestedingsplatform te uploaden als .xls(x)- en .pdf-bestand. Het niet volledig invullen of wijzigen van het Prijzenformulier kan leiden tot uitsluiting van de inschrijving. Het is enkel toegestaan positieve bedragen in te vullen. De prijsopgave dient in Euro's (€) (op twee (2) decimalen) en exclusief BTW te geschieden. Eventuele kortingen moeten verwerkt zijn in uw offerte.

Tenzij uitdrukkelijk anders bepaald in de documenten van de offerteaanvraag zijn prijzen all-in en exclusief BTW. Indexering van aangeboden prijzen is niet mogelijk conform het bepaalde in de Overeenkomst.

De inschrijving die de laagste inschrijfprijs heeft aangeboden, krijgt de maximale score van 100 punten voor de prijs. Alle overige inschrijvers worden gerelateerd aan de inschrijving met de laagste prijs (afgerond op hele punten) middels de volgende formule:

$$\text{Score prijs} = \frac{\text{totaal prijs laagste inschrijving}}{\text{totaalprijs uw inschrijving}} \times 100$$

Bovenstaande geldt ook voor de situatie waarin wordt aangeboden op basis van nacalculatie met plafondprijs. De plafondprijs wordt in dat geval als totaalprijs gebruikt.

De score op prijs telt voor 30% mee.

5. Gunningsmethodiek

De ontvangen offertes worden beoordeeld op 1) het voldoen aan de Raamovereenkomst en 2) het voldoen aan de gestelde minimumeisen. Voldoen de ontvangen offerte(s) aan de Raamovereenkomst en de gestelde minimumeisen en zijn ze evenmin onregelmatig

en/of onaanvaardbaar en/of niet geschikt, dan worden die offerte(s) beoordeeld op de gunningscriteria Kwaliteit. Na ontvangst van het subgunningscriteria Kwaliteit zal deze score in CTM worden gecombineerd met de score voor Prijs.

Er wordt vervolgens wordt gegund op grond van de Economisch Meest Voordelige Inschrijving.

De prijs-/kwaliteitsverhouding is 30%/70%.
De Totaalscore van een Inschrijving wordt daarbij als volgt berekend:

Totaalscore = 30% x score Prijs + 70% x score Kwaliteit

De Inschrijver met de hoogste totaalscore heeft de economisch meest voordelige inschrijving gedaan en eindigt daardoor als 1e in de rangorde.

Alle inschrijvers ontvangen via CTM bericht over de gunningsbeslissing.

De inschrijvers van wie de inschrijving is afgewezen ontvangen in ditzelfde bericht de motivering van de afwijzing, waarbij de naam van de Opdrachtnemer, die de beste prijs-kwaliteitverhouding heeft gedaan, wordt vermeld alsmede de kenmerk(en) en voorde(e)l(en) van de winnende inschrijving ten opzichte van hun eigen inschrijving.

Vanaf de datum van verzending van de gunningsbeslissing wordt voor de overeenkomst wordt gesloten, een wachttijd van vijf (5) werkdagen in acht genomen. Gedurende deze wachttijd is er gelegenheid tot het stellen van vragen en om uw bezwaren ten aanzien van deze gunningsbeslissing kenbaar te maken door betekening van een dagvaarding aan de contactpersonen, VNG Realisatie verzoekt u uw vragen zo vroeg mogelijk te stellen, zodat deze ruim voor het einde van de termijn van vijf (5) werkdagen kunnen worden beantwoord.

Indien na het verstrijken van deze termijn van vijf (5) werkdagen geen bezwaren zijn ingediend, zal de Nadere Overeenkomst worden opgesteld.

Volledigheidshalve wordt daarbij benadrukt dat de (definitieve) gunningsbeslissing geen aanvaarding inhoudt in de zin van artikel 6:217, eerste lid, van het Burgerlijk Wetboek. Dat houdt in, dat tot het moment waarop de Nadere Overeenkomst door Deelnemer en Leverancier in CTM is getekend, de Deelnemer zich te allen tijde het recht voorbehoudt om deze procedure vanwege haar moverende redenen tussentijds te beëindigen. Daarbij kan de betreffende Deelnemer niet aansprakelijk worden gesteld voor door Inschrijver(s) geleden schade of tot een (on)kostenvergoeding worden verplicht door Inschrijver(s). Voorbeelden (niet limitatief) voor het beëindigen van de procedure zijn onder meer de situaties waarin de ingediende aanbiedingen of de gevoerde gesprekken, niet leiden tot een in haar ogen passend aanbod, alsmede de situatie waarin de economisch meest voordelige offerte het budget van de Deelnemer overschrijdt.

6. Reageren?

U kunt uw belangstelling uitsluitend kenbaar maken via het DAS (Dynamisch Aankoop Systeem) waarvan VNG Realisatie gebruikmaakt: http://www.ctmsolution.nl/project/vng-vngrealisatie

Reacties van gecontracteerde opdrachtnemers die niet via dit DAS lopen, worden niet in behandeling genomen.

Na gunning van deze aanvraag, worden ingestuurde documenten (zoals cv en plan van aanpak) van niet gegunde partijen zowel op CTM Solution als intern definitief verwijderd.