Bijlage 1. Begrippen- en afkortingenlijst

Nr.	Omschrijving
1.	**Aanbestedende dienst:** De Belastingdienst.
2.	**Aanbestedingsstukken:** Alle documenten in de aanbestedingsprocedure verwoord in het Beschrijvend Document.
3.	**Aanbestedingswet:** Gewijzigde wet van 2012, geldend vanaf 1 juli 2016, houdende nieuwe regels omtrent aanbestedingen, aangehaald als de Aanbestedingswet 2012, ook wel AW2012 genoemd.
4.	**Aankondiging:** Een publicatie in het Publicatieblad van de EU, via www.tenderned.nl, waarin de opdracht wordt aangekondigd en de markt wordt opgeroepen een Inschrijving in te dienen.
5.	**Acceptatie**: De schriftelijke goedkeuring door de Opdrachtgever, na Oplevering van het Resultaat, van alle onderdelen van de Prestatie, waarna de Prestatie, in de (Productie)omgeving(en) kan worden geplaatst
6.	**Acceptatietest:** De testprocedure van de (nieuw) te leveren Prestatie, waarmee kan worden aangetoond dat, op basis van de Overeenkomst, de geleverde Prestatie, aan de overeengekomen specificaties van Aanbestedingsstukken. Een A&P test kan hiervan onderdeel uitmaken.
7.	**Actieve Deelnemer:** Een Deelnemer die per 12 maanden voortschrijdend, één of meerdere malen (deels) het toetsproces doorloopt.
8.	**Additionele diensten** Dit betreffen aanvullende diensten welke, gedurende de looptijd van de Overeenkomst, door Opdrachtnemer op verzoek van Opdrachtgever op ad-hoc basis worden geleverd. Deze diensten bestaan uit de inzet van consultants. Additionele diensten worden op incidentele basis via inkoopopdrachten aan Opdrachtnemer verstrekt en vergoed op basis van een tarief per uur (tenzij expliciet anders wordt overeengekomen).
9.	**Application Programming Interface (API):** Een set aan definities waarmee softwareprogramma's onderling kunnen communiceren.

10. **Attack and Penetration test (A&P-test):**
Attack and Penetration test (ook bekend als pentest) is een beveiligingstest waarbij de ICT-oplossing, zowel handmatig als geautomatiseerd (bijv. d.m.v. een Vulnerability scan), op de getroffen beveiligingsmaatregelen wordt getest.

    Het type A&P-test is zowel black box (ongeautoriseerd, zonder documentatie) als white box (ook wel aangeduid met crystal box, geautoriseerd met informatie over de ICT-oplossing). De gehele hard-en softwarestack wordt tijdens een A&P test getest. Een broncodereview maakt normaal gesproken ook onderdeel uit van een A&P-test. Bij de A&P test wordt minimaal gebruik gemaakt van de OWASP (Open Web Application Security Project) Top 10 (momenteel versie 2017), STRIDE (Spoofing, Tampering, Repudation, Information disclosure, Denial of service, Elevation of Priviledge) en bekende Kwetsbaarheden uit de CVE (Common Vulnerabilties and Exploits) database.

11. **Audit:**
Een onafhankelijke en/of interne auditdienst betreffende een deskundige beoordeling van kwaliteitsaspecten van de te leveren en geleverde Prestatie. Het betreft een kwaliteitstoetsing ten aanzien van de Prestatie op basis van deze Overeenkomst alsmede ten aanzien van de betrouwbaarheid, beveiliging, vertrouwelijkheid, continuïteit, effectiviteit en efficiency als ook de verplichtingen aangaande het inzet van Personeel en diens onderaannemers, van door Opdrachtnemer aangeboden Prestatie en eventuele locatie(s) van waaruit de Prestatie worden aangeboden. Bij een onafhankelijk deskundige is er sprake van een bindend advies.

12. **Autorisatiebron**
Systeem of applicatie waarmee een gebruiker specifieke rechten krijgt voor de Oplossing.

13. **Backoffice medewerker:**
Een medewerker van de Belastingdienst(Academie) die verschillende rollen kan vervullen, bijvoorbeeld ten aanzien van de ontwikkeling, het beheer van opleidingen en toetsen en het beschikbaar stellen daarvan. Ook bekend onder de namen Functioneel beheerder, Ontwikkelaar, Onderwijskundige, Procescoördinator, Logistiek coördinator, Servicedesk medewerker.

14. **Beschikbaarheid**:
De mate en/of tijd waarin de Diensten gedurende de service window beschikbaar en functioneel dienen te zijn conform de overeengekomen functionaliteit. De overeengekomen Beschikbaarheid wordt uitgedrukt als een percentage. De geplande niet-beschikbaarheid wordt niet meegerekend bij de bepaling van het beschikbaarheidspercentage.

15. **Beschrijvend Document (BD)**:
Het onderhavig document, inclusief Bijlagen, met kenmerk IUC21-017, op basis waarvan de Inschrijver een Inschrijving kan indienen in het kader van de aanbesteding.

16. **Bestelnummer**
Een door de Opdrachtgever verstrekt nummer bestaande uit 10 cijfers (4500 XXXXXX) welke door Opdrachtnemer op de factuur vermeld moet worden. Het Bestelnummer wordt ook wel een 4500-nummer genoemd

17. **Beveiliging:**
De mate waarin de Oplossing in staat is ongeoorloofde toegang - opzettelijk of per ongeluk - tot Gegevens te voorkomen.

18. **Beveiligingsincident:**
Beveiligingsincidenten zijn Incidenten die een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van de Gegevens in informatieverwerkende systemen hebben.

19. **Bijlagen**:
Genoemde Bijlagen in lijst van bijlagen in het Beschrijvend Document en een aanhangsel bij de Overeenkomst dat na parafering door Partijen onderdeel van de Overeenkomst uitmaakt.

20. **BIO:**
Baseline Informatiebeveiliging Overheid: De BIO is een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen). De BIO is volledig gebaseerd op de internationale norm ISO/IEC 27002. Het concretiseert een aantal eisen tot verplichte operationele afspraken (rijksmaatregelen), om een eenduidig minimumniveau van beveiliging voor Gegevens te garanderen. De standaard basisbeveiligingsniveaus (BBN's) met bijbehorende beveiligingseisen maken risicomanagement eenvoudiger.

21. **Blok:**
Een verzameling vragen rondom een bepaald thema, onderwerp of leerdoel.

22. **Calamiteit:**
Een ongeplande situatie waarbij verwacht wordt dat de duur van het niet beschikbaar zijn van de Oplossing de afgesproken drempelwaarden zal overschrijden.

23. **Call:**
Een melding van de Opdrachtgever aan de Helpdesk van Opdrachtnemer waarmee deze het volgende kan aangeven: een Incident, een Probleem, een vraag; een opmerking en een verzoek om ondersteuning, Bevindingen uit een Test en verzoek om ondersteuning bij een verstoring. Ook een melding van een Incident door een medewerker van Opdrachtnemer is een Call.

24. **Conformiteitenlijst:**
Bijlage 16 bij de Aanbestedingsstukken met een overzicht van alle geschiktheidseisen (GE), Vormvereisten (VE) en gunningseisen- (GUE).

25. **Contractmanager**:
De verantwoordelijke voor het vertalen en beheren van de eisen vanuit het bedrijfsproces naar afspraken over de dienstverlening door de ICT-dienstverleners in het kader van de geautomatiseerde informatievoorziening.

26. **Cumulatief voortschrijdend:**

Wanneer bij afrekening per Actieve Deelnemer een hogere staffel wordt bereikt en daarmee een hogere korting geldt, geldt deze hogere korting ook voor de eerder berekende Actieve deelnemers uit dat jaar. Het teveel betaalde dient te worden verrekend aan het eind van elk jaar.

27. **CVE-database:**
Een CVE-database is een database met Common Vulnerabilties and Exploits. In deze database zijn bekende (en aangemelde) Kwetsbaarheden te vinden. Deze Kwetsbaarheden zijn gekwalificeerd middels CVSS.

Databases:

- Mitre: https://cve.mitre.org/cve/
- CVE Details: https://www.cvedetails.com/
- National Vulnerabilities Database (NIST): https://nvd.nist.gov/vuln

28. **Dossier Afspraken en Procedures (DAP):**
Beschrijving van operationele en logistieke procedures, inclusief governance, die als Bijlage E bij de Overeenkomst wordt/is toegevoegd.

29. **Datalek:**
Een inbreuk op de Beschikbaarheid, integriteit en/of de vertrouwelijkheid van (Persoons)Gegevens, waaronder mede wordt verstaan een inbreuk op de Beveiliging conform de vingerende wetgeving op het gebied van de bescherming van (Persoons-) Gegevens.

30. **Deelnemer**:
Een Gebruiker die zich heeft of is ingeschreven voor een toets.

31. **Diensten/Dienstverlening:**
Alle door Opdrachtnemer krachtens deze Overeenkomst te verrichten werkzaamheden zodat de Opdrachtgever de Oplossing conform Specificaties kan gebruiken. Hieronder valt in ieder geval (ten minste) de realisatie van de Oplossing via Implementatie, het gebruik van de Oplossing inclusief Onderhoud, Support en Additionele diensten.

32. **Derde partij:**
Ingeschakelde Opdrachtnemer(s) door Opdrachtgever waarmee Opdrachtnemer op grond van de (beperkte) resultaatverplichting dient samen te werken, bijvoorbeeld, maar niet uitputtend: de aan te wijzen leverancier van een A&P test, TPM of Audit.

33. **Documentatie:**
De door Opdrachtnemer ten behoeve van Opdrachtgever te leveren Documentatie behorende bij de Prestatie, als omschreven in Aanbestedingsstukken en/of nadere overeenkomst en met inbegrip, maar niet beperkt tot, Documentatie op voor computer leesbare media.

34. **Fatale termijn:**
Een nadrukkelijk als zodanig door Partijen overeengekomen termijn bij overschrijding waarvan de Partij ten aanzien van wie de termijn is gesteld onmiddellijk, dat wil zeggen zonder ingebrekestelling, in verzuim geraakt.

35. **Gebruik:**
De Kwaliteit van de performance, presentatie en interactie van de Oplossing.

36. **Gebruiker:**
De Gebruiker is de aanduiding voor een willekeurige functionaris in de Oplossing die geautoriseerd is om gebruik te maken van de Oplossing.

37. **(Persoons)Gegevens:**
Feiten die een waarde of een toestand aanduiden. Gegevens, worden weergegeven door karakters, getallen of symbolen. En betreft in een voorkomend geval een Persoonsgegeven zoals bedoeld in de AVG.

38. **Geplande niet-beschikbaarheid:**
De periodes waarbij de Oplossing, met instemming van de Belastingdienst, niet beschikbaar is.

39. **Helpdesk:**
Loket waar Calls door de Opdrachtgever gemeld kunnen worden gedurende het Service Window.

40. **Identity Management-systeem (IMS):**
Een informatiesysteem of een set van technologieën om een persoon toegang te geven tot de Oplossing.

41.	**Impact:** De mate van invloed van een Incident, Probleem of wijziging op de businessprocessen van de Opdrachtgever. De invloed is een vermindering van de beschikbaarheid in aantallen gebruikers, ICT-services of bedrijfsprocessen die er last van hebben ('hoe ernstig is het'). De Impact wordt als een criterium gebruikt voor het toekennen van de Prioriteit.
42.	**Implementatie:** Alle activiteiten – zoals o.a. benoemd in paragraaf 2.5 van het Beschrijvend Document en hoofdstuk 5 van de Specificatie van Opdracht die gericht zijn op het inrichten van de Oplossing, zodat de Oplossing na Acceptatie conform Specificaties gebruikt kan worden.
43.	**Incident**: Elke gebeurtenis, tijdens de Operationele fase, die niet tot de standaardoperatie van de Prestatie behoort en die een interruptie of een vermindering van de Kwaliteit en Continuïteit van de vereiste dienstverlening veroorzaakt. Het betreft ook een Incident indien er een afwijking geconstateerd wordt t.a.v. de functionele specificaties. Hieronder wordt ook, maar niet limitatief, een gebeurtenis verstaan die valt onder de reikwijdte van het begrip Informatiebeveiliging, waarbij bijvoorbeeld een inbreuk makende gebeurtenis niet leidt tot een interruptie of een vermindering van de kwaliteit en continuïteit van de vereiste dienstverlening.
44.	**Informatiebeveiliging:** Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking van de Prestatie in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
45.	**Inkoopopdracht:** Het elektronische bericht (bijvoorbeeld in de vorm van een document of e-mail) met inbegrip van het Bestelnummer, waarmee onder verwijzing naar de Overeenkomst aan Opdrachtnemer opdracht wordt gegeven om over te gaan tot levering van de Prestatie.
46.	**Inschrijver:** Partij die een Inschrijving indient op basis van het gestelde in de Aanbestedingsstukken.
47.	**Inschrijving:** De aanbieding met begeleidende documenten die de Inschrijver indient bij de Aanbestedende dienst ter beantwoording van het gestelde in Aanbestedingsstukken.
48.	**ISO 27001**: ISO 27001 specificeert eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. Het ISMS is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatie afdoende beveiligen en vertrouwen bieden.
49.	**Koppeling:** Een verbinding die volgens een bepaalde standaard de uitwisseling van Gegevens tussen de Oplossing en een ander informatiesysteem verzorgt.
50.	**Kritieke Performance Indicatoren (KPI's):** Deze Performance Indicatoren zijn essentieel voor het niveau van de dienstverlening van de Opdrachtgever ten aanzien van de Kwaliteit van de Prestatie. Het niet voldoen aan de gestelde eisen leidt tot verminderde Kwaliteit van de dienstverlening, continuïteitsrisico's en/of imagoschade. KPI's worden aangemerkt als Fatale Termijn.

51. **Kwaliteit:**
De mate waarin de Prestatie, in de vorm van Beheer en Onderhoud en Support voldoet aan de overeengekomen functionele eisen en prestatie-eisen volgens Specificaties en die de Opdrachtgever redelijkerwijs mag verwachten en eveneens ziet op het geheel van eigenschappen en kenmerken dat van belang is voor het voldoen aan vastgestelde of vanzelfsprekende behoeften.

52. **Kwetsbaarheden:**
Een (vaak) onbedoelde verzwakking in de beveiliging van een softwarecomponent. Hierdoor lopen Beschikbaarheid, integriteit en/of vertrouwelijkheid van de Oplossing (inclusief haar data) gevaar. Een Kwetsbaarheid is niet noodzakelijkerwijs van technische aard, maar kan ook een organisatorische (procedurele) oorzaak hebben. Kwetsbaarheden kunnen daarnaast een grote impact hebben op het imago van de Belastingdienst. De Belastingdienst onderscheidt de volgende vier typen Kwetsbaarheden: (cyber)hack, responsible disclosure, CVE-database en Security Note en Bevinding uit A&P-testen.

53. **Logbestand:**
Een bestand waarin alle gebeurtenissen van een bepaald proces bijgehouden worden.

54. **Marktconform**
Handelingen of condities die overeenkomstig de gangbare normen binnen de markt zijn.

55. **National Cyber Security Centre (NCSC)**
Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. De missie van het NCSC is het bijdragen aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving.

56. **Natuurlijk Persoon:**
Met deze term worden alle niet-rechtspersonen aangeduid, dit is met name van belang voor de reikwijdte van AVG.

57. **Nota('s) van Inlichtingen:**
Nadere Inlichtingen op het Beschrijvend document, welke integraal deel uitmaken van de aanbestedingsstukken.

58. **Onderhoud:**

Alle activiteiten van Opdrachtnemer gericht op het verbeteren, herstellen, waaronder het uitvoeren van service- en onderhoudswerkzaamheden en/of in aanvaardbare werkbare (operationele) situatie houden van de Oplossing conform het gestelde in de Aanbestedingsstukken. Dit alles met inbegrip van de (eventuele) nieuwe functionaliteiten, gericht op het in operationele staat brengen en houden van de Oplossing, evenals de helpdeskactiviteiten in de vorm van Support.

59. **Opdrachtgever:**
Aanbestedende dienst conform Aanbestedingswet en eveneens de partij ten behoeve waarvan de Overeenkomst wordt gesloten waaronder de BelastingdienstAcademie en SSO.

60. **Opdrachtnemer:**
de partij met wie deze Overeenkomst wordt aangegaan.

61. **Open Standaarden:**
Een open standaard (of norm) is publiekelijk beschikbaar. De specificaties van de standaard mogen vrij van licentierechten worden toegepast, gebruikt en gehanteerd.

De term wordt vooral gebruikt bij hard- en software, omdat juist daar ook veel gesloten standaarden worden gebruikt, waarbij men voor de inzage van de specificaties, een licentie dient aan te vragen.

62. **Operationele fase**:
De fase na integrale Acceptatie waarin Opdrachtnemer de Oplossing operationeel houdt, innoveert en verbetert tot het moment van Retransitie.

63. **Oplossing:**
Het gebruik, en hiermee het 24/7 beschikbaar stellen van het Toetssysteem in de vorm van een SAAS met inbegrip van Implementatie en Onderhoud en Support.

64. **Overeenkomst**:
de Overeenkomst met Bijlagen en inbegrip van (eventuele) addenda en inkoopopdrachten.

65. **Partijen:**
De Opdrachtgever en de Opdrachtnemer tezamen.

66. **Persoonsgegevens:**
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Wederpartij in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

67. **Plan van Aanpak:**
Een gedetailleerd voorstel dat de uit te voeren activiteiten en benodigde resources beschrijft om tot een bepaald doel te komen.

68. **Prestatie**:
De Oplossing tezamen met de Additionele diensten.

69. **Prij(s)zen** De, in Euro's, overeengekomen vergoeding voor de te verrichten Prestatie door Opdrachtnemer neergelegd in bijlage 10 - het Prijzenformulier van de Aanbestedingsstukken.

70. **Prioriteit**:
Categorie voor het aangeven van het relatief belang van een Call. De Prioriteit hangt af van de Impact en Urgentie, en wordt gebruikt om de benodigde tijd vast te stellen waarbinnen actie moet worden ondernomen.

71. **Probleem of Problem:**
Een oorzaak van een of meerdere Incidenten, waaraan een structurele fout in de Dienst ten grondslag ligt.

72. **Pseudonimiseren:**
Bij pseudonimisering kunnen gegevens met de juiste sleutel inzichtelijk gemaakt worden, waardoor herleiding naar natuurlijke personen weer mogelijk is. Anonimisering draait daarentegen om versleuteling die niet omkeerbaar is: als persoonsgegevens eenmaal zijn ontdaan van identificerende data, is het niet meer mogelijk om deze later weer met personen in verband te brengen.

Het verschil tussen geanonimiseerde en gepseudonimiseerde gegevens is belangrijk omdat de AVG niet van toepassing is op volledig geanonimiseerde data. Voor gepseudonimiseerde data gelden de regels uit de AVG nog wel.

73. **Reactietijd Incident/ Vraag (ook wel Responsetijd):**
De tijd tussen melding van een Incident/vraag en het moment dat gestart wordt met het oplossen c.q. beantwoorden van een Incident/vraag.

74. **Release(s):**
Een (verzameling van) Dienst(en), met inbegrip van de benodigde systeemprogrammatuur, datadefinities en tabelvullingen die als geheel zal worden geaccepteerd. In een Release kunnen één of meerdere (hot)fix-es, wijzigingen of vernieuwingen verwerkt zijn.

75. **Release notes:**
De Release notes beschrijven bij oplevering de wijzigingen ten opzichte van vorige versies, de bekende problemen (en hun Workarounds) en instructies voor Installatie en gebruik.

76. **Resultaat**:
De van te voren door de Opdrachtgever en Opdrachtnemer overeengekomen Prestatie die door Opdrachtnemer aan Opdrachtgever ter Acceptatie wordt aangeboden.

77. **Retransitie:**
Het geheel van handelingen en maatregelen nodig om te voorzien van een overgang van de Prestatie van de ene Opdrachtnemer naar een eventuele andere/nieuwe Opdrachtnemer van de Opdrachtgever.

78. **Roadmap:**
Een indicatieve planning voor toekomstige ontwikkelingen waarin globaal is aangegeven welke ontwikkeling wanneer beschikbaar komt.

79. **Recovery Point Objective (RPO)**
De, in GUE 88 (Bijlage A), beschreven maximale hersteltijd van 24 klokuren.

80. **Recovery Time Objective (RTO)**
Afgesproken herstelpuntdoelstelling/ per saldo het maximaal toelaatbare dataverllies (= de back-up-frequentie).

81. **Service Level Agreement (SLA):**
Bijlage van de Inschrijving dat na parafering door Partijen onderdeel van de Overeenkomst uitmaakt. Het betreft een beschrijving van de vastgestelde normen in de vorm van Service Levels voor de Prestatie en Additionele dienstverlening.

82. **Service Levels:**
Ten behoeve van de Prestatie en Additionele dienstverlening overeengekomen vormen van dienstverlening in de Overeenkomst met inbegrip van de Aanbestedingsstukken en Specificaties en eveneens nader uitgewerkt in de SLA als onderdeel van de Overeenkomst.

83. **SOC:**
Het Security Operations Center (SOC) van de Belastingdienst is verantwoordelijk voor de beveiliging van het datacenter en infrastructuur van de Belastingdienst. Daarnaast is het aanspraakpunt voor melding van beveiligingsincidenten van buiten de Belastingdienst in gebruikzijnde ICT-oplossingen.

Het SOC heeft ook als taak Vulnerability scans op zowel on-als off-premise gehoste ICT-oplossingen uit te voeren en mee te werken aan A&P-testen.

84. **Specificaties (van de opdracht):**
Het onderdeel van de Aanbestedingsstukken met gunnings-, uitvoeringseisen en wensen ten aanzien van de Prestatie.

85. **SSO O&P:**
Shared Service Organisatie - Organisatie en Personeel.

86. **Statement of Applicability:**
Een Statement of Applicability (SoA) is een integraal onderdeel van de implementatie van NEN-EN-ISO/IEC 27001. Het geeft aan welke maatregelen een organisatie gebruikt om risico's te identificeren (met doorverwijzing naar relevante documentatie), waarom deze geselecteerd zijn, of deze geïmplementeerd zijn en waarom de overige maatregelen niet worden gebruikt.

87. **Stekkermandaat**:
Het recht van de Opdrachtgever om “de stekker uit het systeem te trekken”. Het Stekkermandaat is gedelegeerd aan het SOC. Naast onbereikbaar maken van de Oplossing moeten de Gegevens van de Opdrachtgever veilig gesteld en onbereikbaar voor derden gemaakt worden.

88. **Support:**
Ondersteuning bieden aan de Opdrachtgever conform de bepalingen zoals neergelegd in de SLA als onderdeel van de Overeenkomst**.**

89. **Third Party Memorandum:**
Een verklaring afgegeven door Opdrachtgever aan te wijzen Derde partij waaruit blijkt dat de opzet, bestaan en werking van de Dienst(en) voldoen aan de gestelde Specificaties of welke maatregelen genomen zijn opdat deze daaraan weer voldoen.

90. **Toetssysteem**:
De software die het digitale toetsproces ondersteunt. Het uitgangspunt is dat in principe elke medewerker binnen de Aanbestedende dienst in de toekomst een toets kan afnemen om zijn/ haar kennis te testen en inzicht te krijgen in de verbeterpunten Dit systeem bestaat ten minste uit een of meer van de volgende componenten (niet-limitatief): auteursomgeving, afspeelomgeving, (toets)analysetool en itembank.

91. **Two-factor Authenticatie:**
Er zijn verschillende vormen van authenticatie die eventueel gecombineerd kunnen worden oom een hoger of lager niveau van beveiliging op te leveren. Daarbij zijn 3 vormen van bewijs bruikbaar:

    - Iets wat je weet (kennis)
    - Iets wat je bezit
    - Iets wat je bent (persoonlijke eigenschap)

    Om de betrouwbaarheid van de authenticatie te vergroten, wordt authenticatie afgedwongen door toepassing van multifactor.

92. **Wensen:**
Wensen zijn onderdeel van de gunningscriteria, de scores op de wensen bepalen per Inschrijving de hoogte van het onderdeel kwaliteit in de prijs/kwaliteit verhouding.

93. **Werkdagen:**
Kalenderdagen behoudens weekenden, algemeen erkende feestdagen en voor personeel van de Opdrachtgever verplichte vrije dagen tussen vrije feestdagen (brugdagen). Opdrachtgever kan eisen dat gedurende feestdagen en weekenden door Opdrachtnemer werkzaamheden worden verricht conform Werkdagen mits dit door de Opdrachtgever tijdig vooraf is aangegeven.

94. **Zero-client footprint:**
Er is, naast een webbrowser, geen additionele software, browser-plugin of additionele hardware nodig op de gebruikersapparaten om alle gevraagde functionaliteit van de Oplossing te kunnen benaderen.