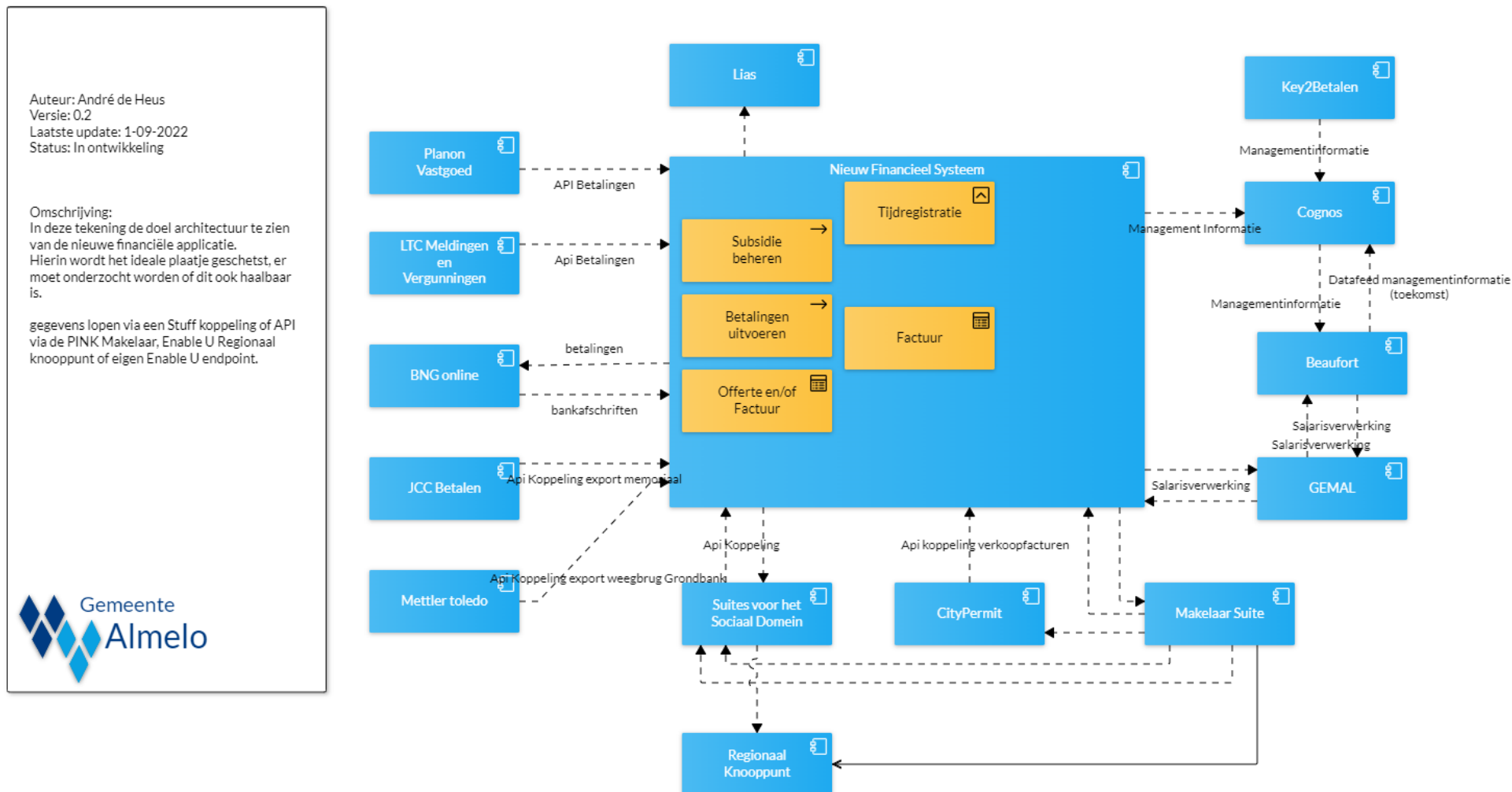


Annex X B SOLL Situatie financieel systeem

Een schematische weergave van een deel van het financiële systeem.

In de tabel is een overzicht van de huidige koppelingen met Decade en de toekomstige situatie.



Koppelingenoverzicht Decade en nieuwe financiële systeem:

pakket	Type verkeer	huidig	Toekomst
Planon Vastgoed	Verkoopfacturen	Excel upload sheet	Automatische koppeling via api
LTC Meldingen en vergunningen	Verkoopfacturen	Excel upload sheet	Automatische koppeling via API
BNG Online	Betalingen, Afschriften	Sepa.xml en BNG.mt940, ABN.mt940	Automatische koppeling via API
JCC betalen	Export Memoriaal	Excel upload sheet	Automatische koppeling via API
Mettler Toledo	Verkoopfacturen	Excel upload sheet	Automatische koppeling via API
Suites voor het Sociaal Domein	memoriaal	Excel upload sheet	Automatische koppeling via API
Citypermit	Verkoopfacturen	Excel upload sheet	Automatische koppeling via API
Lias	Management informatie	Datakoppeling Lias (sql scripts)	Automatische koppeling via API
Donau Factuur	inkoopfacturen	PL/SQL van en naar Decade	Automatische koppeling via API of pakket vervangen door nieuwe financiële applicatie
DigiData suite invoice	Herkenning en routing inkoopfacturen	PL/SQL van en naar Decade	Automatische koppeling via API of pakket vervangen door nieuwe financiële applicatie
COGNOS	Management informatie	Rechtstreekse DB koppeling	Voor management informatie koppelen via Datadump of datasets op termijn API operationele rapportages binnen de applicatie.
Pink Makelaar	BRP Verzorgt de StUF XML koppelingen	Rechtstreeks StUF	Rechtstreeks API BRP aangevuld met KVK
Raet HR Core online	memoriaal	Via Gemal en Pentaho/cognos	Automatische koppeling via API??
Stratech SBA	subsidiebetaalopdrachten	Digidata invoice en Donau	Automatische koppeling via API of applicatie vervangen LET OP: Kansendossier!
Decos Join	Archief DMS	Bestaat nog niet	Automatische koppeling via StUF/API
Leerzaam (huidig Civision wordt vervangen)	Betaalopdrachten leerlingvervoer	Bestaat nog niet, Civision een SEPA-XML bestand wordt gegenereerd, die handmatig via het web-portaal van de BNG wordt geupload.	Automatisch via API

Bijlage Beveiligingseisen:

1	Inschrijver dient, eventueel met behulp van onderaannemers die de rekencentraservices van de inschrijver verzorgen, in het bezit te zijn van een geldig ISO 27001 certificaat (bij voorkeur organisatorisch geïmplementeerd conform de controls van ISO 27002) of aantoonbaar gelijkwaardig. Als gelijkwaardig wordt erkend een ander keurmerk en/of een verklaring, uitgebracht door een onafhankelijke instantie die voldoet aan de Europese normenreeks voor certificering, waarmee de inschrijver aantoont volledig te voldoen aan de gestelde eisen die ten grondslag liggen aan het gevraagde certificaat. Voeg een geldig certificaat en een toepassingsverklaring aan uw inschrijving toe of een ander keurmerk/verklaring die gelijkwaardig is aan ISO 27001.
2	In aanvulling op eis 12: De oplossing functioneert voor wat betreft aspecten van beveiliging en privacy volledig conform alle betreffende wet- en regelgeving (ten minste AVG en BIO), en andere van toepassing zijnde wetgeving, tenzij door de inschrijver nadrukkelijk anderszins in de inschrijving aangegeven. De BIO voldoet uiteraard enkel voor de reikwijdte die redelijkerwijs aan een SaaS-leverancier kan en behoort te worden gesteld. Wij verwijzen in dit kader expliciet naar die BIO-eisen waarbij in de kolom "Verantwoordelijke" (ondermeer) de "Dienstenleverancier" wordt benoemd.
3	Inschrijver conformeert zich, uiteraard met de reikwijdte van de opdrachtscope en de eigen inschrijving hierop, gedurende de looptijd van de overeenkomst + 12 maanden na afloop, volledig aan alle voor de opdracht relevante standaarden die door het Forum Standaardisatie op de lijst 'veelgebruikte open standaarden' of 'open standaarden voor pas toe of leg uit' zijn geplaatst. De te realiseren koppelingen / webservices / berichtuitwisselingen voldoen aan de landelijke standaarden (www.istandaarden.nl, Vektis, Vecozo, Zorg Instituut Nederland, VNG Realisatie).
4	De aspecten van beveiliging en privacy zijn in grote mate geborgd door de vereiste compliancy door wet- en regelgeving (AVG en BIO), de vereiste certificeringen ten aanzien van de inschrijver (ISO27001 en ISO 9001:2008 of 2015 of gelijkwaardig) en de toepasbaarheid van de GIBIT 2020. Vanuit deze context is het Twente Regio toegestaan te auditeren op beveiligingsaspecten ten aanzien van de aangeboden oplossing. Echter, bij voorkeur wordt compliancy door inschrijver pro-actief aangetoond aan de hand van een geldig te behouden ISO27001-certificering gedurende de gehele looptijd. Voor de jaarlijkse ICT-beveiligingsassessment ten aanzien van DigiD volstaat een Third Party Mededeling (TPM), die voldoet aan de Logius richtlijnen. Alle kosten rondom het aantonen van compliancy vallen ten deel aan de inschrijver en dienen in de inschrijving opgenomen te zijn. Alleen bij gerede twijfel ten aanzien van de beveiliging en privacy zal Twente Regio haar auditrecht uitoefenen.

5	De applicatie voldoet aan de eisen van "Star level 1 continuous" van de Cloud Control Matrix v4 van de cloud security alliance: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/
6	De applicatie ondersteunt TLS 1.3 met betrekking tot de API-koppelingen voor gegevensuitwisselingen.
	De API is getest en beveiligd tegen de dreigingen van de OWASP-API-security top 10 https://apisecurity.io/encyclopedia/content/owasp/owasp-api-security-top-10-cheat-sheet.htm
7	Het systeem biedt een procedure voor het verwijderen van data/informatie (Niet zijnde Exit strategie).
8	Opgeslagen documenten en gegevens moeten na het verstrijken van de bewaartermijn op een gecontroleerde en efficiënte manier vernietigbaar zijn.
9	De oplossing voldoet aan NEN-ISO 23081 en NEN-ISO 15489
10	De gegevens, documenten en metadata-(kenmerken) zijn te allen tijde overdraagbaar naar de opvolger van de (toekomstige) applicatie/SAAS- of Cloud-oplossing. Ook bij faillissement van de leverancier/het bedrijf dat de SAAS- of Cloudoplossing levert.
11	Dataportabiliteit moet mogelijk zijn voor de inhoud (waarden) van de data in de ICT Prestatie alsmede de bijbehorende metadata bestaande uit ten minste de beschrijving van de betekenis van entiteiten, relaties, attributen en waardenbereik.
12	Het technische formaat voor dataportabiliteit is een open formaat, en sluit bij voorkeur aan bij de XML- of JSON-standaarden. Indien aan het bovenstaande niet voldaan kan worden en ander gangbaar technisch dataformaat wordt gebruikt, dient de meta-informatie afzonderlijk gedocumenteerd te worden.
13	Leverancier geeft de specificaties voor dataportabiliteit. Deze specificaties voor dataportabiliteit bevatten voor de export én import van data tenminste: a. de beschrijving van betekenis van de data van entiteit, attributen en waardebereik; b. de beschrijving van betekenis en relaties (kardinaliteit) tussen gegevens; c. het formaat waarin data kan worden geëxporteerd/geïmporteerd; d. welke gegevens en metadata wel en niet worden meegenomen en het formaat waarin dat plaatsvindt; e. de beschrijving van de import en exportfunctionaliteit die het softwareproduct ondersteunt; f. de data die niet in de import en export meegenomen wordt omdat deze geen eigendom is van Opdrachtgever; g. opgave van de technische formaten die voor dataportabiliteit gebruikt worden.
14	De gegevens/documenten binnen de SAAS-/Cloud-oplossing worden binnen de Europese Unie opgeslagen op een datacentrum/Cloudserver en de leverancier/eigenaar van de SAAS-/Cloud-oplossing is (bij voorkeur) een Europees bedrijf.
15	Het systeem ondersteunt toegang tot gegevens door middel van een autorisatiesysteem op basis van rollen en rechten.
16	De oplossing heeft importmogelijkheden en exportmogelijkheden vanuit functionele behoefte.
17	De oplossing heeft import- en exportmogelijkheden in gangbare dataformaten (bij voorkeur XML) tbv een exit- of migratiestrategie.

18	De applicatie ondersteunt veilig inloggen door SSO door middel van OAuth en SAML en federatie met Azure AD.
19	De oplossing heeft een mogelijkheid om vastgelegde autorisaties op alle niveaus inzichtelijk te maken per persoon, per gebruikersgroep en rol. Hiervoor is het toegepaste autorisatieschema te exporteren naar een bestand, dat leesbaar en interpreteerbaar is voor derden (zoals toezichthouders zoals bijvoorbeeld de accountant, auditors, etc.).
20	De oplossing biedt zodanige functionaliteit m.b.t. auditing/logging dat van alle relevante handelingen en pogingen daartoe voor wat betreft processen, processtappen en statuswijzigingen - zowel door gebruikers als de oplossing zelf - door middel van logging een historie wordt vastgelegd (van welke handelingen en pogingen daartoe, wanneer en door wie zijn uitgevoerd). Deze auditing/logging dient zonder tussenkomst van de leverancier door functioneel en daartoe geautoriseerde gebruikers bekeken te kunnen worden.
21	Het systeem dient een audittrail van de proces- en gebruikersacties vast te leggen.
22	Het systeem dient alle handelingen vast te leggen in een logging. Deze logging blijft een half jaar bewaard.
23	Het systeem dient de integriteit van logging te waarborgen.
24	Ingeval van een SAAS-oplossing dient de beschikbaarheid van het systeem gegarandeerd te zijn op minimaal 99% per maand tijdens kantoortijden 08.00 – 17.00 uur). Dit is zeer laag, wat komt er uit de dataclassificatie als eis?)
25	In geval van een SAAS-oplossing is de software en bijbehorende data geïnstalleerd en opgeslagen in een in de Europese Economische ruimte gevestigd datacenter, vallend onder Nederlands of Europees recht.
26	De SaaS-omgeving biedt de mogelijkheid om de aanwezige data te exporteren in een gangbaar formaat (bij voorkeur XML). Dit ter facilitering van een exit-strategie en in verband met een datawarehouse behoefte.
27	De applicatie kan koppelen (gegevens uitwisselen) met andere applicaties door middels moderne API's en via onze API-Gateway (2Secure/Layer7)
28	De applicatie ondersteunt TLS 1.2 met betrekking tot het beveiligen van de webapplicatie in de browser (het "slotje")
29	De applicatie ondersteunt TLS 1.3 met betrekking tot de API-koppelingen voor gegevensuitwisselingen.
30	Leverancier past de hardening richtlijnen van het NIST toe
31	Alle verplichte relevante beveiligingsstandaarden van het forum standaardisatie zijn toegepast. Leverancier garandeert dat dit zo blijft bij wijzigingen van deze standaarden gedurende de looptijd van het contract, zie voor de huidige lijst: https://www.forumstandaardisatie.nl/open-standaarden/verplicht?trefwoord=172 . IPv6 en IPv4 worden ondersteund.
32	De databasebeheerder mag geen inzage hebben in de opgeslagen gegevens van de deelnemers.
33	Medewerkers van de leverancier mogen geen toegang hebben tot de data van de deelnemers.

34	Het is mogelijk de test omgeving op te zetten door de productie omgeving te kopiëren zonder daarbij de persoonsgegevens uit de productie omgeving mee te kopiëren, of waarbij persoonsgegevens uit de productieomgeving worden gepseudonimiseerd.
35	Leverancier laat jaarlijks een pentest op de broncode van de software uitvoeren en verhelpt de bevindingen van deze pentest binnen 3 maanden na het doen van de bevinding.
36	Er zijn maatregelen genomen om de applicatie te beschermen tegen DDOS aanvallen.
37	Koppelingen dienen beveiligd te zijn.
38	Er wordt jaarlijks een pentest uitgevoerd op alle deelnemer omgevingen. Hierbij wordt gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Leverancier heeft een proces voor het uitvoeren van de verbeterpunten, montort hierop en rapporteert hierover aan de opdrachtgever.
39	Beheerportalen mogen niet zonder beperkingen worden blootgesteld, dat wil zeggen alleen benaderbaar zijn vanaf vast te leggen IP adressen en toegang wordt verleend na twee factor authenticatie.
40	Het is mogelijk de applicatie logging te koppelen aan het SIEM van een deelnemer.
41	De leverancier heeft maatregelen genomen voor het beheer van technische kwetsbaarheden (BIO 12.6.1). Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.
42	De basisbeveiliging van de applicatie is op orde volgens test van internet.nl.
43	De basisbeveiliging van de mailcomponent is op orde volgens test van internet.nl
44	De webinterface van de applicatie is beveiligd tegen de OWASP-top 10 en leverancier garandeert dat dit gedurende de looptijd van het contract zo blijft.
45	Data at rest (ook de back-up) en data in transit wordt versleuteld volgens de geldende standaarden gedurende de looptijd van de overeenkomst. Voor in transit is dit op dit moment TLS 1.2 en TLS 1.3, voor data at rest Advanced Encryption Standard (AES)-256.
46	Transport versleuteling voldoet aan de "Guidelines for quantum-safe transport-layer encryption" https://www.ncsc.nl/documenten/publicaties/2022/juli/guidelines-for-quantum-safe-transport-layer-encryption/guidelines-for-quantum-safe-transport-layer-encryption
47	De oplossing is Digitoegankelijk volgens EN 301 549 met WCAG 2.1, https://forumstandaardisatie.nl/open-standaarden/digitoegankelijk-en-301-549-met-wcag-21
48	De inschrijver is zonder enig voorbehoud verantwoordelijk voor backup, restore, recovery en uitwijk met betrekking tot de gehele oplossing. Hierbij geldt een Recovery Point Objective van maximaal 24 uur en een Recovery Time Objective van maximaal 4 uur.
49	Restore moet mogelijk zijn op document niveau, maar ook op niveau van vangnet en van alle gegevens van een deelnemer.

50	Om de gehele oplossing in relatie tot haar technische omgeving op een juiste wijze te kunnen onderhouden en beheren, wordt de oplossing up-to-date en compliant gehouden op ten minste de laatste en de twee voorlaatste versies voor alle gerelateerde programmatuur (ook wel N-2 voor alle vereiste programmatuur, bestaande uit (client)middleware, databaseprogrammatuur (server en client), servers en hun besturingssystemen, virtualisatietechnieken, etc.), zodanig dat de vermelde functionaliteiten gedurende de gehele contractduur in stand gehouden worden, tenzij partijen om wat voor reden schriftelijk iets anders overeenkomen. Inschrijver zal, uiterlijk binnen 12 maanden na het beschikbaar komen van nieuwe versies, de aanpassingen van de oplossing hiervoor beschikbaar stellen. De inschrijver mag tot deze tijd 1 versie achterlopen).
51	Voor het uitvoeren en afhandelen van niet-standaard wijzigingen, levert inschrijver voor de start van de uitvoering een plan van aanpak en een raming voor de eventuele kosten en doorlooptijd. Pas na akkoord van de opdrachtgever op dit plan van aanpak zal inschrijver zijn werkzaamheden starten.
52	Nieuwe releases moeten er in ieder geval voor zorgen dat de functionaliteit, zoals beschreven in deze aanbestedingsdocumentatie, gebruikt kan blijven worden. Nieuwe releases mogen dus niet leiden tot een verminderde functionaliteit of het niet meer kunnen voldoen aan de eerder hieraan gestelde eisen en wensen.
53	Nieuwe releases worden standaard voorzien van releasenotes vooraf, welke minstens 5 werkdagen voorafgaand aan de release worden verstrekt aan de gemeente. De releasenotes omvatten ten minste: instructiemateriaal, informatie over eventuele impact op koppelingen, informatie over eventuele impact op certificaten en informatie over gewijzigde functionaliteit.
54	Nieuwe releases worden standaard uitgerold op de testomgeving. Deze kunnen in geval van releasefunctionaliteit die beduidende impact heeft op het gebruik, verplichte configuratie activiteiten van de gemeente vergt of niet standaard gedeactiveerd is, met een termijn van minimaal 10 werkdagen worden getest en geaccepteerd, alvorens de release wordt uitgerold naar de productieomgeving. Bij productie belemmerende bevindingen wordt, totdat adequaat herstel en het testen hiervan heeft plaatsgehad, gezamenlijk een uitrolmoment bepaald.
55	Het wijzigingen- en releasebeheer omvat eveneens het uitbrengen van impact analyses op basis van business requirements. Het betreft hier algemeen advies over een adequaat gebruik en beheer van de aangeboden oplossing in relatie tot management- en gebruikers- en beheersbehoeften van de Twente Regio en wijzigingen hierin.
56	De inschrijver verzorgt een helpdesk, welke als 'single point of contact' dienst doet voor het stellen van vragen, melden van incidenten en indienen van wijzigingsvoorstellen, alsook voor informatie over de afhandeling daarvan. De helpdesk is telefonisch bereikbaar van 8.00 uur tot 18.00 uur op werkdagen (maandag tot en met vrijdag met uitzondering van officiële feestdagen). Buiten deze tijden wordt een calamiteitenregeling door inschrijver beschikbaar gesteld (van toepassing zijnde op de incidenten met prioriteit TOP zoals onderstaand beschreven). In de SLA geeft inschrijver de omgang, respons- en oplostijden aan voor aangemelde incidenten. Daarbij wordt tevens de calamiteitenregeling beschreven. Uiteraard wordt hierbij geen afbreuk gedaan aan ondergestelde eisen.

57	De helpdesk is ook beschikbaar via internet (webportaal of e-mail). Vragen, meldingen van incidenten en wijzigingsvoorstellen kunnen op alle dagen 24 uur per dag online worden ingediend (formulier). Dergelijke online vragen, meldingen van incidenten en wijzigingsvoorstellen worden automatisch per mail bevestigd en daarmee geregistreerd. Tevens kan de voortgang van deze incidenten en wijzigingsmeldingen digitaal worden geraadpleegd en gevolgd.
58	Op basis van de urgentie en impact onderscheidt inschrijver in ieder geval drie prioriteiten voor incidenten en andersoortige meldingen (vragen, verzoek om informatie, service requests), te weten hoog, midden en laag. Naast bovenstaande prioriteiten is er een categorie 'TOP' welke van toepassing is voor incidenten waarbij de dienstverlening van Regio Twente (of de processen) ernstige hinder ondervindt (webportalen niet-beschikbaar, voor beheerders niet-beschikbaar), waarbij de informatieveiligheid in het gedrang komt of waarbij doorwerken in de oplossing leidt tot schade aan de oplossing of de data. Bij het indienen van een melding of incident is de gemeente altijd leidend in de bepaling van de prioriteit van de melding en daarmee zelfstandig sturend voor de onderstaand beschreven reactie-, oplos- en statusupdate-tijden.
59	In het proces tussen het optreden van een incident en de definitieve oplossing onderscheidt inschrijver in ieder geval de volgende begrippen met bijbehorende definitie: Responstijd: de maximale tijd tussen het indienen van een melding en het versturen van de ontvangstbevestiging door inschrijver. Reactietijd: de maximale tijd tussen het indienen van een melding tot het aannemen van de melding door één van de oplosgroepen van inschrijver. Oplostijd: de maximale tijd tussen het indienen van een melding en het aanbieden van een oplossing (bij incidenten en wijzigingen) of het beantwoorden van een vraag. Statusupdate tijd: de maximale tijd tussen het indienen van een melding en de eerste statusupdate, of tussen de voorgaande statusupdate en de meest recente statusupdate. In de SLA die onderdeel vormt van de overeenkomst worden vermelde tijden nader ingevuld.
60	De oplossing voldoet aan NEN-ISO 23081 en NEN-ISO 15489

61	Het systeem ook aan de eisen van de archiefwet voldoen
----	--

Naast bovenstaande beveiligings-eisen moeten er ook processen worden ingericht die het functioneren van de koppelingen bewaken.

De eisen hebben niet alleen betrekking op de koppelingen, maar hebben betrekking op de applicatie.

Bij elke koppeling of uitwisseling is de vraag: kan de andere huidige applicatie leveranciers het ook leveren. Dit zal in de POC fase uitgezocht worden.

We standaardiseren zoveel mogelijk op StUF, er is echter geen standaard voor financiële systemen beschikbaar. Daarom is een moderne API wenselijk. Bij API koppelingen moet er een goede beschrijving bekend zijn, en deze moet backwards compatible zijn.

Medio 2023 komt er een intern API-platform, meer informatie is hier nog niet over beschikbaar.

Daarnaast hebben we de applicatie JCC Betalen Externe betalingen. Hiermee worden komen de betalingen via de internetkassa in JCC Betalen terecht. Een mogelijke oplossing is dat externe betalingen in JCC Betalen geregistreerd worden en JCC de export levert richting de nieuwe financiële applicatie.

- Zonder twee-factor authenticatie dienen wachtwoorden te bestaan uit minimaal 14 vrij te kiezen karakters en complex. Bij meer dan 20 karakters vervalt de complexiteitseis.
- Wachtwoorden zijn maximaal een jaar geldig indien de (informatie)-systemen voldoen aan het wachtwoord beleid. Anders zijn de wachtwoorden maximaal 6 maanden geldig.
- Na vijf foutieve inlogpogingen wordt een lockout tijd van 60 minuten actief. Na deze lockout tijd wordt de teller van verkeerd wachtwoord weer gereset naar nul.
- Wachtwoordhistorie wordt ingesteld op 10 woorden, dat wil zeggen dat 10 opeenvolgende wachtwoorden telkens verschillend moeten zijn.
- Systeembeheerders wordt alleen toegang verleend op basis van twee-factor authenticatie. SMS als tweede factor is niet toegestaan.
- Wachtwoorden van systeemaccounts zijn minimaal 20 posities lang en complex.

- Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onderandere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
- Er wordt een lijst bijgehouden met woorden en combinaties van tekens die niet in het wachtwoord mogen voorkomen. Gemeente Almelo kan aan deze lijst items toevoegen.