



Bijlage 4 Gunningstest

Openbare Europese aanbesteding

Customer Identity and Access Management (CIAM)

Kadaster

Kenmerk	A24-103908
Opdrachtgever	Directie BOI
Auteur	Niels Stoker
Versie	1.0
Versiedatum	12-03-2024



Datum
03-11-2021

Titel
Beschrijvend Document:
CCaaS
Kenmerk: xxx

Blad
2 van 13

Inhoud

1	Inleiding	3
2	Plaats en periode van de gunningstest	3
3	Gunningstest	3
4	Uitvoering en beoordeling	3
5	Gunningstest cases	4
5.1	Onboarding	4
5.1.1	Inleiding	4
5.1.2	Context	4
5.1.3	Nieuwe klant (organisatie)	4
5.2	In- en uitloggen	7
5.3	Gebruikersbeheer (selfservice)	8
5.3.1	Inleiding	8
5.3.2	Context (proces en applicatie)	9
5.3.3	Aanmaken- en uitnodigen nieuwe gebruiker	10
5.3.4	Inloggen nieuwe gebruiker	12



Datum
03-11-2021

Titel
Beschrijvend Document:
CCaaS
Kenmerk: xxx

Blad
3 van 13

1 Inleiding

Het Kadaster hecht een groot belang aan het beproeven van CIAM voordat daadwerkelijk tot gunning wordt overgegaan. Het gaat hier om het verifiëren van de juistheid en waarheidsgetrouwheid van de Inschrijving. Met de gunningstest wordt aangetoond dat een aanbieder voldoet aan de uitvraag van het Kadaster.

Dit betekent concreet dat wordt gecontroleerd of aan vooraf bepaalde eisen kan worden voldaan. Aangezien het Kadaster SaaS-diensten afneemt, gaat het Kadaster ervan uit dat in de basis alle aangeboden functionaliteiten kunnen worden getoond. De gunningstest wordt uitgevoerd na de voorlopige gunning.

2 Plaats en periode van de gunningstest

De gunningstest zal plaatsvinden op een Kadaster vestiging. Inschrijver dient beschikbaar te zijn op de genoemde data in paragraaf 3.3. Van Inschrijver wordt verwacht dat de noodzakelijke technische en personele ondersteuning aanwezig is.

3 Gunningstest

Indien de Inschrijver niet slaagt voor de gunningstest, zal diens aanbieder terzijde worden gelegd, aangezien is komen vast te staan dat deze niet voldoet aan de geteste gunningseisen. Het Kadaster zal vervolgens mogelijk bepalen wie alsdan voor gunning in aanmerking komt. In dat geval zullen de behaalde punten van de overgebleven Inschrijvers op de gunningscriterium kwaliteit niet wijzigen. De formule voor de berekening voor de punten van het gunningscriterium prijs worden opnieuw berekend aan de hand van de overgebleven Inschrijvers. Daarna wordt de uitslag op basis van de nieuwe puntentelling opnieuw vastgesteld, om zo de nieuwe nummer 1 te kunnen selecteren en uitnodigen voor een (eventuele) gunningstest.

4 Uitvoering en beoordeling

Om te komen tot een test waarbij de nadruk ligt op integratie/operabiliteit en toepasbaarheid van de functionaliteit van de aangeboden oplossing, zal zowel Kadaster als de aanbieder inspanning moeten leveren en is samenwerking essentieel. De eindresultaten van de testen zijn niet allesbepalend; het tot stand komen van een integrale oplossing binnen een bepaald tijdsbestek, is ook een wezenlijk onderdeel van de beoordeling.

De casussen uitgewerkt in dit document zijn richtinggevend en in gezamenlijk overleg kan bepaalt worden, wat de beste oplossing is voor de test en welke delen er binnen het gestelde tijdsbestek haalbaar zijn.

De gunningstest vindt plaats na voorlopige gunning, zie paragraaf 8.1 van het Beschrijvend document (BD). De leden van het projectteam beoordelen de gunningstest individueel. Het projectteam zal een gezamenlijke sessie houden waarbij de definitieve beoordeling en motivatie worden vastgesteld.

5 Gunningtest cases

5.1 Onboarding

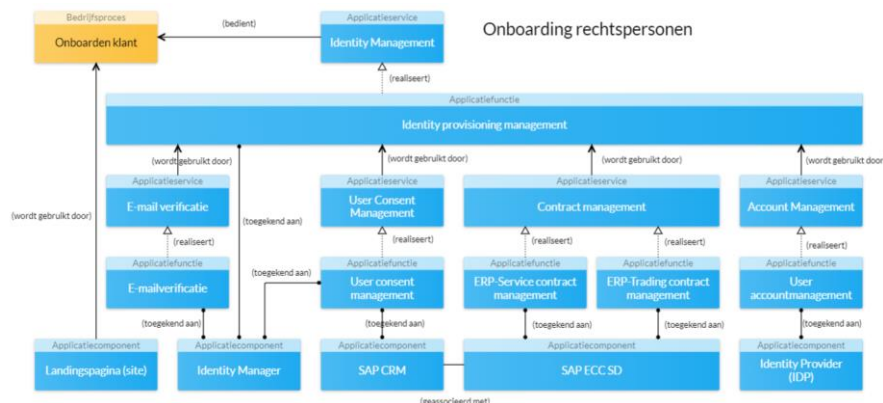
5.1.1 Inleiding

Met deze casus wil Kadaster toetsen hoe de aangeboden oplossing invulling geeft aan het (digitaal) klant- worden proces. Kadaster ziet twee uiterste gevallen van de oplossing:

1. Onboardingsproces wordt volledig geleid door CIAM functionaliteit
2. Onboardingproces wordt volledig geleid door Kadaster functionaliteit

De realiteit zal in het midden liggen waarbij Kadaster gevoel wil hebben van de positionering van de CIAM functionaliteit en de noodzakelijke kennis en effort om de integratie tussen de bestaande Kadaster omgeving en de CIAM SAAS te realiseren en beheren.

5.1.2 Context

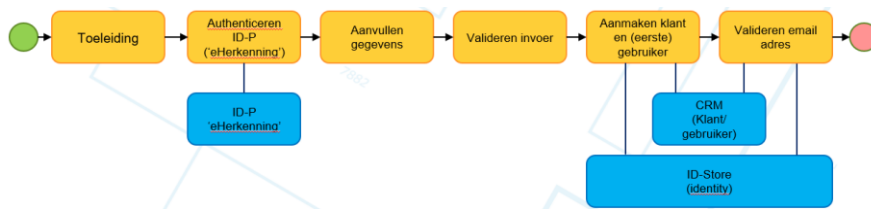


Figuur 1: Onboarding en doel applicatieve ondersteuning

Figuur 1 is overgenomen uit de doelarchitectuur met betrekking tot het klant (organisatie) worden proces. Wanneer de achterliggende processen verder worden ontleed, kunnen en aantal subprocessen onderscheiden worden die in deze test gebruikt kunnen worden.

5.1.3 Nieuwe klant (organisatie)

In dit proces wordt een nieuwe zakelijke klant opgevoerd. Hiervoor voorziet Kadaster in de basis een volledig ('STP') geautomatiseerd proces waarbij de rechtspersoon zich identificeert met een door Kadaster vertrouwd authenticatiemiddel, 'ID-P eHerkenning'. Dit middel hoeft niet eHerkenning te zijn, maar zou het in de praktijk wel kunnen zijn:



Figuur 2: Klant- worden proces (globaal)

START conditie

- Potentiële klant nog niet geregistreerd
- CRM (SAP) systeem of stub beschikbaar voor het aanmaken van organisaties en contactpersonen/gebruikers
- CIAM (test) service beschikbaar met werkende federatie naar ID-P
- Bestaand, werkend ID-P test-account, 2FA

PROCES

Toeleiding

Webpagina waarin de potentiële klant wat informatie krijgt over het klant worden en kan kiezen voor het starten van de registratie.

Test: Afhankelijk van de aangeboden oplossing kan de webpagina door een Kadaster front-end worden aangeboden of is het een pagina die wordt uitgeserveerd door CIAM en waarvan de opmaak (CSS) van Kadaster wordt gehanteerd.

Authenticeren ID-P ('eHerkenning')

Potentiële klant moet zich identificeren door in te loggen met een bekende ID-P (federatie). Hierop komt en tenminste een unieke identifier beschikbaar voor het vervolg van het proces wordt geprefilled (in de praktijk bij eHerkenning zou dit het KvK nummer en de Handelsnaam van een organisatie kunnen zijn). In Figuur 2 wordt open gelaten hoe de federatie met eHerkenning loopt. Kadaster gebruikt hiervoor de ID-P broker van Signicat waarbij de Layer-7 gateway een intermediaire rol heeft.

Aanvullen gegevens

Potentiële klant kan aanvullende gegevens invullen:

1. Naam organisatie
2. Adres
3. Contactpersoon (/ 'beheerder')
4. Emailadres contactpersoon

Tijdens de proef kan in overleg bepaald worden welke details cq aanvullende gegevens van toepassing moeten zijn.



Datum
03-11-2021

Titel
Beschrijvend Document:
CCaaS
Kenmerk: xxx

Blad
6 van 13

Valideren invoer (optioneel)

Ihkv prioritering van de test, kan deze stap eventueel overgeslagen worden, maar de stap beoogt het testen van het valideren van de ingevoerde data en het geven van een passende melding om de invoer te corrigeren wanneer deze niet correct is. Een huisnummer moet bijvoorbeeld primair een getal zijn.

Aanmaken klant en (eerste) gebruiker

De test hier is het kunnen aanspreken van een extern systeem. CRM in dit geval. Kadaster zou hiervoor het bestaande SAP CRM willen inzetten die via SAP PO een API aanbiedt. Eventueel kan dit systeem vervangen worden door een stub die een API biedt die de ingevoerde data accepteert en een Klant-ID van de organisatie retourneert en een Gebruiker-ID van de (eerste) gebruiker van de organisatie. Vervolgens wordt de digitale identiteit van de klant (organisatie) aangemaakt en van de eerste gebruiker met respectievelijk het klant-ID en het gebruikers-ID als foreign keys. De gebruiker krijgt als entitlement tenminste de rol 'beheerder'.

Valideren emailadres gebruiker

In de test is tot nu toe uitgegaan van een bestaande externe ID-P en bijbehorende identificerende gegevens. Er is voor de gebruiker geen noodzaak een Kadaster account aan te maken, dus het eerder gebruikte middel is leidend voor de identificatie. Het valideren van het emailadres is een optie die Kadaster wel graag als losse functie zou willen kunnen gebruiken, maar ziet dit voor deze test tevens als optioneel.

Er wordt door de aangeboden CIAM oplossing een verificatiemail gestuurd naar het opgegeven emailadres waarin een link/knop is opgenomen waarmee de ontvanger het mailadres bevestigt.

EIND conditie

- Klant en gebruiker opgevoerd in 'CRM'
- Klant en gebruiker digitale identiteiten aangemaakt
- Gebruiker heeft tenminste de rol 'beheerder'
- Optioneel: emailadres van de gebruiker is gevalideerd

Controle uitkomsten:

1. Primair: zie use case paragraaf 5.2
2. Secundair (alternatief): inzien logs/data CRM en CIAM
3. CIAM faciliteert de flow en vanuit de flow kunnen subflows gestart worden en/of externe apps aanroepen
4. Samenwerking; tot stand komen van de opzet en de resultaten

Nr.	Eis
23	Kadaster kan binnen de CIAM oplossing het onboardingsproces zelf vormgeven (flow, condities, data- en datavalidatie) en operationaliseren.
24	Onboardingsfuncties worden ook via een API aangeboden.
25	Onboardings (proces) logica kan koppelen met externe bronnen.
29	Verificatie van klantgegevens, zoals e-mail en telefoonnummer moet mogelijk zijn tegen door Kadaster configureerbare condities (beheer/configuratie functie)

93	Wens: De oplossing past standaard op de beschreven (PVA: Figuur 16) koppelvlakken of biedt hiervoor een alternatief. In dit geval SAP CRM (koppeling 3)
----	---

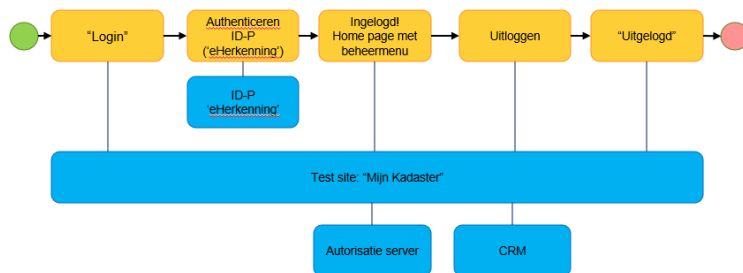
5.2 In- en uitloggen

START conditie

Use case paragraaf 5.1 uitgevoerd en succesvol afgerond

PROCES

Nieuwe gebruiker kan met ID-P inloggen op een ("Mijn Kadaster") testsite waarbij de beheerfuncties worden getoond (rol 'beheerder') en de opgeslagen gegevens in CRM:



Figuur 3: In- en uitloggen proces

Login

Webpagina met 'login' knop/optie voor de gebruiker

Authenticeren ID-P "eHerkenning"

Inloggen met bestaande middel wat ook gebruikt is voor onboarding. Ook hiervoor geldt dat de bestaande federatie met eHerkenning via de ID-P Broker van Signicat loopt en vanuit Kadaster door de Layer-7 gateway wordt gefaciliteerd.

Ingelogd! Homepage met beheermenu

Webapplicatie toont zeer basale homepage:

1. Beheerfunctie(s) (hieruit blijkt dat de gebruiker de beheerder rol heeft)
2. Klant- en gebruikersinformatie uit CRM wordt getoond
3. Uitloggen knop/link

Uitloggen

Keuze 'uitloggen' op homepage waarna de sessie wordt beëindigd en de gebruiker een bevestiging krijgt van uitgelogd te zijn.

Uitgelogd



Datum
03-11-2021

Titel
Beschrijvend Document:
CCaaS
Kenmerk: xxx

Blad
8 van 13

Sessie beëindigd; browse-back brengt de gebruiker niet terug naar de homepage, maar naar de loginpagina (start vh proces).

EIND conditie

1. Gebruiker (beheerder) uitgelogd

Controle uitkomsten:

1. In- en uitloggen met federatie succesvol
2. Basale autorisatie op basis rol (beheerder)
3. Tonen gegevens externe bron (-SAP- CRM)

Nr.	Eis / Wens
43	Eis: CIAM ondersteunt meerdere ID-P's (inlogmiddelen) op basis van federatie volgens standaarden zoals SAML-2 en OIDC.
45	Wens: Het gebruik van meerdere ID-P's tegen condities kan geconfigureerd worden; beschrijf hoe dit werkt
52	Eis: autorisatie kan gelaagd worden opgebouwd waarbij het bestaande 2-laags model (toegang tot dienst en toegang binnen dienst) wordt ondersteunt.

5.3 Gebruikersbeheer (selfservice)

5.3.1 Inleiding

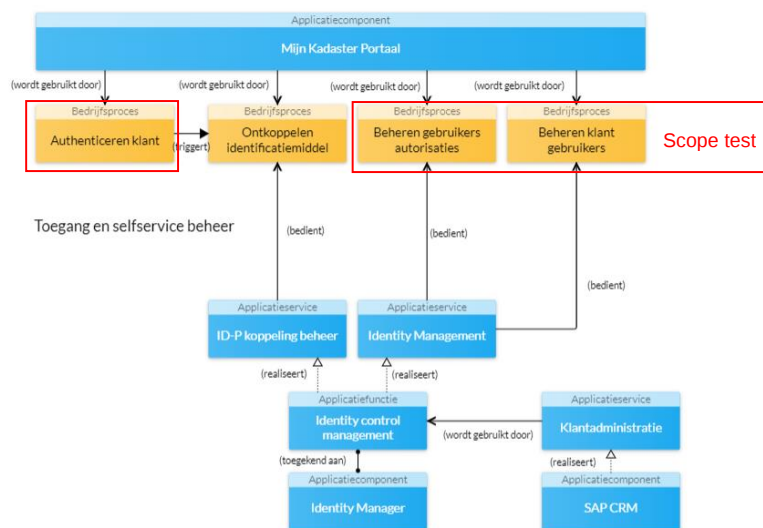
Met deze casus wil Kadaster toetsen hoe de aangeboden oplossing werkt voor de ondersteuning van gebruikers (selfservice) beheer.

Ook hiervoor ziet Kadaster twee uiterste gevallen van de oplossing:

1. Web front-end en controller logica valt volledig binnen Mijn-Kadaster waarbij CIAM een API biedt voor identiteit beheer
2. CIAM biedt volledig configurabel beheer selfservice functionaliteit waarbij Kadaster de opmaak aanlevert

Kadaster wil gevoel wil hebben van de positionering van de CIAM functionaliteit en de noodzakelijke kennis en effort om de integratie tussen de bestaande Kadaster omgeving en de CIAM SAAS te realiseren en beheren.

5.3.2 Context (proces en applicatie)



Figuur 4: Gebruikersbeheer en doel (SOLL) applicatieve ondersteuning

Figuur 4 is overgenomen uit de doelarchitectuur met betrekking tot het verkrijgen van toegang tot- en het uitvoeren van selfservice beheer functionaliteit.

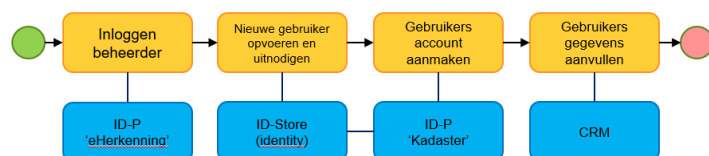
In paragraaf 5.2 is het inloggen (authenticeren) en uitloggen van de beheerder reeds getest. Aanvullend zal in deze test gekeken worden of een nieuw aangemaakte gebruiker en bijbehorend account in de Kadaster ID-P werkt en de gebruiker daadwerkelijk kan inloggen en toegang krijgt tot toegekende functies. De test gaat uit van twee rollen; 'beheerder' en 'gebruiker'.

5.3.3 Aanmaken- en uitnodigen nieuwe gebruiker

START conditie

Use case paragraaf 5.1 uitgevoerd en succesvol afgerond.

PROCES



Figuur 5: aanmaken, uitnodigen en bevestigen nieuwe gebruiker

Inloggen beheerder

Zie use case paragraaf 5.2, deel 1 (inloggen beheerder). Beheerder logt in en heeft door de beheerrol toegang tot het (gedelegeerd) gebruikersbeheer.

Nieuwe gebruiker opvoeren en uitnodigen

Beheerder selecteert 'nieuwe gebruiker aanmaken' binnen de gebruikersbeheer functionaliteit.

Invoervelden voor het opvoeren van een nieuwe gebruiker worden getoond. Voorstel:

1. Emailadres (gebruikersnaam)
2. Rechten: standaard (rol gebruiker)

Voor de gebruiker wordt binnen cq gerelateerd aan, een nieuwe digitale identiteit aangemaakt met het ID van een prematuur gebruikersaccount (ID-P Foreign Key). Naar het opgegeven e-mailadres wordt een uitnodigingsmail gestuurd met een link waarmee de gebruiker de onboarding zelf verder kan verzorgen. Beheerder ziet de aangemaakte nieuwe gebruiker met bijpassende status ('uitgenodigd' oid).

Gebruikersaccount aanmaken

Geïnitieerd door de vorige stap is er een prematuur gebruikersaccount aangemaakt welke door de beoogde gebruiker definitief gemaakt moet worden:

1. Wachtwoord invoeren volgens policy
2. Tweede factor (2FA) instellen; TOTP en SMS (backup)

Na succesvol afronden van account, wordt ook de status van de gebruiker geupdate ('afgerond' oid) zodat de beheerder dit ook kan zien.



Datum
03-11-2021

Titel
Beschrijvend Document:
CCaaS
Kenmerk: xxx

Blad
11 van 13

Gebruikersgegevens aanvullen

Aanvullen van persoonsgegevens (naam, email) en eventuele toestemming gebruik/opslag gegevens door de gebruiker zelf. E-mailadres moet afwijkend kunnen zijn van het emailadres van het account en indien afwijkend, moet het emailadres geverifieerd kunnen worden door een email te sturen naar het opgegeven emailadres met een verificatielink.
Gegevens worden opgeslagen in 'CRM' systeem via een API.

EIND conditie

1. Gebruikers identiteit aangemaakt met de rol 'gebruiker' gerelateerd aan de klant (organisatie)
2. Gebruikersaccount aangemaakt met foreign key relatie naar gebruikersidentiteit
3. Gebruikerstatus 'definitief' of 'actief'
4. CRM bijgewerkt; nieuwe gebruiker binnen klantorganisatie met toestemming en gevalideerd emailadres

Controle uitkomsten:

1. Aanmaken en uitnodigen nieuwe gebruiker (identiteit, persoonsgegevens, account)
2. Toekennen gebruikers (basis) rol door beheerder (rol)
3. Operationeel (werkend) account met autorisatie volgens basisrol
4. Optioneel: Aangemaakt contactpersoon 'CRM' voor wegschrijven persoonsgegevens

Met opmerkingen [EL1]: We kunnen een eenvoudige API maken ('Hello World') die een valide accesstoken vraagt en dan kunnen we ook een PEP meenemen (GAA?)

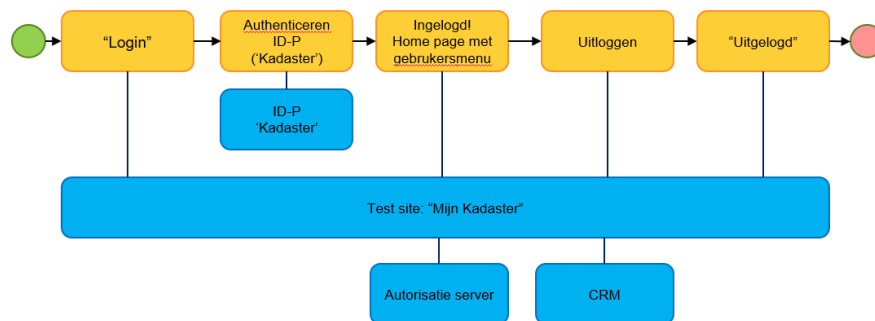
Nr.	Eis / Wens
63	Eis: Voor het beheren van gebruikers binnen selfservice biedt CIAM zoek, selecteer, inzien, aanmaken en wijzigen functionaliteit (CRUD) middels API(s) en -optioneel- web-GUI
64	Eis: CIAM biedt de mogelijkheid om verschillende (beheer)rollen te onderscheiden met verschillende autorisaties
66	Eis: de beheerder kan eigen (beschikbare) rechten aan gebruikers toekennen en weer intrekken
67	Eis: de beheerder kan gebruikers aanmaken en uitnodigen voor onboarding
70	Eis: de beheerder kan onboarding aanvragen inzien

5.3.4 Inloggen nieuwe gebruiker

START conditie

Use case paragraaf 5.3.3 uitgevoerd en succesvol afgerond.

PROCES



Figuur 6: inloggen (nieuwe) gebruiker

“Login”

Gebruiker kiest “login” knop of link op de toeleidingspagina van de Mijn Kadaster testapplicatie. Gebruiker kiest voor inloggen met Kadaster account.

Authenticeren ID-P (‘Kadaster’)

Gebruiker login in met 2FA

“Ingelogd!” Home page met gebruikersmenu

Na succesvol authenticeren wordt het gebruikersmenu getoond (afwijkend van het beheerdersmenu) en worden de eerder ingevoerde gebruikersgegevens getoond welke zijn opgehaald uit ‘CRM’.

Uitloggen

Gebruikers kiest ‘uitloggen’ functie waarmee de sessie wordt beëindigd en onderliggend(e) token(s) worden gedevalideerd. “Uitgelogd” pagina wordt getoond; browse back leidt de gebruiker naar het login scherm.

EIND conditie

1. Gebruiker uitgelogd

Controle uitkomsten:

1. In- en uitloggen met Kadaster ID-P 2FA
2. Optioneel: validatie ingevoerde gegevens door uitgenodigde gebruiker
3. Optioneel: aanroepen ‘CRM’ (SAP CRM Kadaster indien haalbaar binnen timebox)
4. Optioneel: lookup CRM persoonsgegevens op basis van foreign key binnen identity



Datum
03-11-2021

Titel
Beschrijvend Document:
CCaaS
Kenmerk: xxx

Blad
13 van 13

Nr.	Eis / Wens
43	Eis: CIAM ondersteunt meerdere ID-P's (inlogmiddelen) op basis van federatie volgens standaarden zoals SAML-2 en OIDC.
56	Eis: CIAM ondersteunt autorisatie op basis van attributen (ABAC) en rollen (RBAC)
58	Eis: CIAM biedt een configureerbaar standaard web-GUI waarvan de opmaak aangepast kan worden (CSS) conform Kadaster-stijl en WCAG compliant gemaakt kan worden.