DE REPUBLIEK DER ZEVEN FACULTEITEN

Vettingmethodiek en beheer voor de Radboud Universiteit

Radboud Universiteit

Bachelorscriptie Security Management

Door: Mitchell Rhemrev (411580)

Scriptiebegeleider: Dr. S Stronks, Msc

Tweede beoordelaar: Rob van Nuland

18 maart 2019

Titelblad

Naam:	Mitchell Rhemrev
Studentnummer:	411580
Afstudeerperiode:	Juni 2018 tot en met maart 2019
E-mailadres:	411580@student.saxion.nl
Telefoonnummer:	+31 6 22 56 83 96
Titel van de afstudeeropdracht:	De Republiek der Zeven Faculteiten.
Naam van de organisatie:	Radboud Universiteit
Adres:	Houtlaan 4, 6525 XZ Nijmegen
Praktijkcoach:	Harrie Harings
Eerste lezer:	Sara Stronks
Tweede lezer:	Rob van Nuland

Voorwoord

Voor u ligt de scriptie “De Republiek der Zeven Faculteiten”. Het onderzoek voor deze scriptie naar de passende vettingmethodiek en het bijbehorende beheer is uitgevoerd bij het ICT Servicecentrum (ISC) van de Radboud Universiteit, te Nijmegen. Deze scriptie is geschreven in het kader van mijn afstuderen aan de opleiding “Security Management” bij Saxion te Apeldoorn en in opdracht van stageorganisatie Radboud Universiteit. Van 25 juni 2018 tot 1 maart 2019 was ik bezig met het onderzoek en het schrijven van de scriptie.

Samen met mijn praktijkcoach en schoolcoach heb ik de onderzoeksvraag voor deze scriptie ontwikkeld. Het onderzoeksproces moest een aantal keer aangepast worden door de hoeveelheid nieuwe en daarmee niet voorziene ontwikkelingen die zich in deze periode hebben voorgedaan. Na een uitgebreid kwalitatief onderzoek en vele uren overleggen met mijn collega’s bij het ISC, heb ik een concreet aanbevelingsrapport kunnen opleveren.

Graag wil ik graag mijn begeleiders Harrie Harings van het ISC en Sara Stronks bedanken voor de goede begeleiding en hun ondersteuning tijdens mijn afstuderen. Ook wil ik alle respondenten bedanken die mee hebben gewerkt met het onderzoek en veel informatie hebben gegeven. Zonder hun input had ik dit onderzoek nooit kunnen voltooien.

Tot slot wil ik graag al mijn collega’s hier bij het ISC bedanken voor de fijne samenwerking. Ik wil specifiek Jan en Marijn hierbij bedanken.

Jan, bedankt voor de gezellige tijd die ik heb gehad met jou op ons kantoor. Je hebt me niet alleen geholpen met de vele vragen die ik had over de organisatie, je hebt me ook veel geleerd over verschillende ICT- termen, systemen en begrippen. Maar je hebt me niet alleen veel geleerd over het zakelijke leven, je hebt mijn kennis enorm uitgebreid over zaken als voedsel, de bio-industrie, fitness, bio-wetenschap en film.

Marijn, zonder jou was dit onderzoek nooit geslaagd. Je kennis over vettingmethodieken en inzet voor de implementatie van twee-factor-authenticatie is van onschatbare waarde. Jij hebt me op het juiste spoor gezet en tot op het laatste moment bijgestaan met input en nieuwe ideeën en je was altijd bereid om met mij te sparren over de vettingmethodieken en bijbehorende organisatie. Je ongebreidelde enthousiasme voor het project heeft mij enorm gemotiveerd om een mooi adviesrapport op te stellen. Ik weet niet hoe ik je ooit voldoende hiervoor kan bedanken.

Ik wens u allen veel leesplezier toe!

Mitchell Rhemrev

Amsterdam, 18 maart 2019

Management Samenvatting

Dit onderzoek is gedaan in opdracht van de Radboud Universiteit. De doelstelling van de afstudeeropdracht was om door middel van kwalitatief onderzoek en praktijkvoorbeelden de vettingmethodiek te identificeren die paste binnen de organisatorische randvoorwaarden van de Radboud Universiteit en aanbevelingen te geven over hoe het beheer en uitvoering hiervan verantwoord belegd kon worden. De probleemstelling die gebruikt is voor het onderzoek was als volgt: *Welke vettingmethodiek past binnen de organisatorische randvoorwaarden van de Radboud Universiteit?*

De Radboud Universiteit wil twee-factor-authenticatie (2FA) implementeren op reguliere applicaties zoals email, Virtual private network (eduvpn) en Osiris (studentadministratie) en belangrijke applicaties zoals beheerservers bij het ISC. Het probleem was dat er nog geen efficiënte manier was om de medewerkers te authentiseren. Daarnaast was het niet helder wat de beveiligingsvoorwaarden waren en welke wensen de gebruikers hadden over de uit te kiezen vettingmethodiek. Om de probleemstelling te beantwoorden werden de volgende onderzoeksvragen gebruikt:

1. *Wat zijn de organisatorische randvoorwaarden voor de vettingmethodiek, van zowel security- als gebruikerskant, van de Radboud Universiteit?*
2. *Welke normen zijn relevant voor de vettingmethodiek van de Radboud Universiteit?*
3. *Welke van de vettingmethodieken uit het rapport "Remote Vetting for SCSA" scoort het hoogst bij de toetsingscriteria van de Radboud Universiteit?*
4. *Hoe voert het Windesheim de vettingprocedure van hun medewerkers uit en hoe is hun beheer hiervan ingericht?*

Om de onderzoeksvragen te beantwoorden werd er een kwalitatief onderzoek uitgevoerd. Om onderzoeksvraag 1 en 2 te beantwoorden zijn er een twee interviews gehouden met de Chief Information Security Officer (CISO) en de Project Manager 2FA van het ISC. Bij onderzoeksvraag 2 werd documentanalyse gebruikt om de genoemde normen uit het interview met de CISO verder uit te zoeken en te bekijken op toepasbaarheid. Onderzoeksvraag 3 is beantwoord door middel van een documentanalyse, het rapport "Remote Vetting for SCSA" is daarvoor onderzocht en de best beoordeelde vettingmethodieken uit het rapport zijn beoordeeld met de toetsingscriteria van de Radboud Universiteit. Onderzoeksvraag 4 werd beantwoord door een interview te houden met collega-instelling het Windesheim te Zwolle.

Aan de hand van de resultaten uit onderzoeksvraag 1 en 2 is een checklist opgesteld waarmee de vettingmethodiek die het best heeft gescoord in onderzoeksvraag 3 getoetst kon worden en uit deze controle is naar voren gekomen dat **SURFsecureID** het beste past binnen de organisatorische randvoorwaarden van de Radboud Universiteit. Om het de gebruikers zo makkelijk als mogelijk te maken om zich te laten vetten, moeten er meerdere RA-punten opgericht worden. Het zou verstandig zijn om alle faculteiten te voorzien van één of maximaal twee RA's. Tevens kunnen werknemers die problemen hebben met de Tiqr-app of hun Yubikey hier langs gaan om dit op te laten lossen. Het advies is om de vettingprocedure door de Personeel & Organisatie (P&O) afdeling binnen de faculteiten uit te laten voeren voor de werknemers van deze faculteit waarbij tevens de faculteitseigen communicatiemiddelen ingezet worden. Daarnaast dient er een promotiecampagne gehouden te worden waarin de noodzaak van zowel twee-factor-authenticatie als de vettingmethodiek en bijbehorende vettingprocedure uitgelegd wordt.

Inhoudsopgave

Begrippenlijst:

Afkortingen:

2FA:

Twee-factor-authenticatie.

BSN:

Burger service nummer.

CvB:

College van Bestuur.

P&O:

Personeel en Organisatie.

RA:

Registration Authority

RAA

Registration Authority Administrator

Begrippen:

Organisatorische randvoorwaarden:

Organisatorische randvoorwaarden zijn eisen waaraan moet worden voldaan om een specifiek proces te kunnen laten plaatsvinden. De organisatie geeft de grenzen aan die men tijdens het uitvoeren van het proces niet mag overschrijven en vormen zo een kader waarbinnen het proces plaats kan vinden (Ensie, 2013).

SURF:

SURF is de ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland. Dankzij SURF beschikken studenten, docenten en onderzoekers in Nederland over de best mogelijke ICT-voorzieningen voor toponderzoek en talentontwikkeling.

Tiqr:

SURF heeft het open-source-authenticatiemechanisme Tiqr ontwikkeld. Hiermee kunnen gebruikers veilig en makkelijk inloggen op online applicaties door een QR-code te scannen met hun telefoon. Ze hoeven geen (eenmalig) wachtwoord en gebruikersnaam meer in te vullen.

Token:

Een token is een elektronisch authenticatiemiddel. Het kan een applicatie op de telefoon zijn als Tiqr of Google Authenticate, of het kan een apparaat zijn dat er uitziet als een sleutelhanger en voorzien is met een drukknop, zoals een Yubikey. Door op de knop te drukken, wordt een eenmalige cijfercode gegenereerd die op het beeldscherm van een computer wordt weergegeven. Dit wordt het One Time Password (OTP) genoemd. Dit OTP wordt gebruikt om in te loggen op bepaalde applicaties, zoals SURFconext of OSIRIS. Het token is verbonden aan één specifiek persoon en dient ter authenticatie van de gebruiker.

Vetting/Vetten:

Een achtergrond onderzoek van een person om te controleren of de persoon ook daadwerkelijk diegene is als wie hij zich voordoet.

Vettingmethodiek:

Een methode of werkwijze, bijvoorbeeld iDIN of DigiD, om de identiteit van een persoon te controleren. Bevat een vettingprocedure en regels voor beheer.

Vettingprocedure:

Het proces wat een gebruiker moet doorlopen om zijn identiteit te laten controleren.

Yubikey:

De Yubikey van Yubico AB is een authenticatie sleutel voor eenvoudige en veilige toegang tot applicaties, netwerken en online services. De Yubikey is een goedkope hardwarematige 2FA-sleutel die eruit ziet als een kleine USB stick.

Hoofdstuk 1

1.1 Inleiding:

De Radboud Universiteit is één van de grootste universiteiten van Nederland, gelegen in Nijmegen. De universiteit telt volgens de laatste telling in oktober 2017 20.967 studenten en 4.921 FTE leden van het personeel (Radboud Feiten & Cijfers, 2017). De Universiteit heeft een breed aanbod van opleidingen, waaronder 37 bachelor programma's en 76 master programma's. (Radboud feiten & cijfers, 2018)

Alle medewerkers en studenten van de Radboud Universiteit voeren hun werk uit op de campus en/of vanaf elders en hebben daarvoor toegang nodig tot de benodigde hulpmiddelen. Het kan de fysieke toegang betreffen tot een laboratorium, maar het zal vaak gaan om toegang tot webservices en diverse ict-diensten, waarbij het soms om gevoelige data kan gaan. Het spreekt voor zich dat het verlenen van toegang op een veilige, d.w.z een gecontroleerde en identificeerbare wijze moet gebeuren waarbij de kans op fouten minimaal is. Dit laatste en specifiek de controle van de identiteit van een persoon aan wie een toegangsmiddel tot gevoelige ict-services of data verleend wordt, is onderwerp van het onderzoek.
Het onderzoek is uitgevoerd in het ICT Service Centrum van de Radboud Universiteit. Het ICT Service Centrum (ISC) levert alle voorzieningen die nodig zijn om de campus te voorzien van hoogwaardige ICT diensten, zoals het netwerk (glasvezel/koper), alle computers voor onderwijs- en onderzoeksystemen, bedrijfsapplicaties en kantoorautomatisering, informatiemanagement advies en ondersteuning, een deskundige helpdesk voor alle medewerkers en studenten, ICT-beveiliging advies en -ondersteuning, applicatieontwikkeling en -beheer, hostingfaciliteiten voor omliggende (academische) ziekenhuizen en telefonie. De centrale IT-organisatie telt 155 medewerkers, deels parttime. Het aantal fulltime medewerkers komt neer op 135 FTE. Het ISC bevindt zich binnen de afdeling "Radboud Services". In bijlage 1 is het organogram van de Radboud Universiteit weergegeven.

De Radboud Universiteit kampt met het probleem dat de digitale identiteit van alle gebruikers binnen de Universiteit alleen met een combinatie username/wachtwoord konden worden geverifieerd. Deze methode wordt als zwakste vorm van verificatie gezien (Hulsebosch, 2017). Een username en password combinatie heeft twee nadelen: ze zijn makkelijk te achterhalen door phishing[1] of door iets simpels als slingerende papiertjes met gegevens van slordige werknemers die zich niet aan de clean-desk policy[2] houden (Hulsebosch, 2017). Als een kwaadwillend individu deze middelen in handen heeft kan hij gemakkelijk de accounts van de gedupeerden misbruiken aangezien er niet meer nodig is dan enkel een username en wachtwoord (Hulsebosch, 2017). Bij de Radboud Universiteit komt dit ook voor en betekent het dat kwaadwillende personen, zoals boze studenten of ontevreden werknemers/docenten, gemakkelijk de persoonlijke gegevens van de persoon achter een account kunnen bereiken en zelfs tentamencijfers kunnen aanpassen.

De Radboud Universiteit wilde niet meer dat docenten de cijfers op Brightspace (de elektronische leeromgeving) publiceerden, omdat het niet duidelijk vermeld was hoe de betreffende docent tot dit cijfer was gekomen en omdat deze nog aangepast kunnen worden. In 2017 was het bijvoorbeeld bekend geworden dat studenten met een simpel trucje in het email-systeem van de Radboud Universiteit een studentnummer konden koppelen aan een naam. Accounts op Brightspace werden

[1] Phishing is een vorm van internetfraude, waarbij de dader mensen probeert op te lichten door ze te lokken naar valse (bank)websites en hen daar te laten inloggen met hun username/password of creditcardnummer. De fraudeur ontvangt dan deze gegevens. (Handbook of Information Security, 2010)
[2] Clean-Desk-Policy is een organisatorische maatregel waarbij alle werknemers hun bureaus aan het einde van de werkdag opgeruimd dienen achter te laten. (Dekantoorvakhandel.nl, 2018)

hierdoor niet meer anoniem en dat was ook een gevaar voor de privacy van de student[3]. Daarom werd er overgestapt naar het invoeren van cijfers in Osiris. Osiris is een Studie Informatiesysteem waarin behaalde resultaten voor tentamens en projecten staan. Zodra een cijfer ingevoerd is in Osiris, kan deze ook niet meer gemakkelijk aangepast worden. Als een cijfer aangepast moet worden, moet de docent dit schriftelijk aanvragen en concreet aangeven wáárom er een aanpassing nodig is.

Deze situatie is dan ook de aanleiding van dit onderzoek, de Radboud Universiteit wil op korte termijn overstappen van het eerdergenoemde één-factor-authenticatiesysteem naar een twee-factor-authenticatiesysteem voor het inloggen op reguliere applicaties zoals mail, eduvpn en Osiris en belangrijke applicaties zoals beheerservers. Twee-factor-authenticatie (kortweg 2FA) is een veiligere manier van inloggen (SURF, 2018). De identiteit van de persoon als gebruiker wordt hierbij vastgesteld door middel van twee factoren. De gebruiker opent het digitale slot niet met één sleutel (één factor), maar met twee sleutels. Dit betekent dat naast het invoeren van een gebruikersnaam en wachtwoord, nog een tweede factor vereist is. Dit kan in de vorm van een SMS dat naar de telefoon van de gebruiker gestuurd wordt. Maar een vingerafdruk of QR-scan kunnen ook als een tweede factor dienen (Hulsebosch, 2017). Om te zorgen dat 2FA betrouwbaar is moet vooraf het 2FA inlogproces al bij de indiensttreding van werknemers en docenten, een identiteitscontrole plaatsvinden om ervoor te zorgen dat de identiteit van diegene die gebruik wil maken van 2FA geauthentiseerd is (Hulsebosch, 2017). Deze identiteitscontrole wordt uitgevoerd door middel van een vettingmethodiek. Een vettingmethodiek is een systeem wat een gebruiker authentiseert. Voorbeelden van vettingmethodieken zijn iDIN, DigiD of Google Authenticate (Hulsebosch, 2017). Een vettingmethodiek bestaat uit twee onderdelen, namelijk de vettingprocedure, oftewel de stappen die de gebruiker moet volgen om zijn identiteit te authentiseren, en regels voor het beheer van de persoonsgegevens. De Radboud Universiteit wil weten welke vettingmethodiek past binnen hun organisatorische randvoorwaarden en hoe het beheer van deze vettingmethodiek ingericht moet worden.

Deze vettingprocedure en het beheer hiervan konden niet zonder zorgvuldige voorbereiding worden opgesteld. Tijdens het onderzoek was het belangrijk om ervoor te zorgen dat de vettingmethodiek compliant was aan de geldige wet- en regelgevingen en werd vormgegeven conform de normenkaders van de Radboud Universiteit. Daarnaast was het van groot belang om de relevante wetgevingen te onderzoeken aangezien er gewerkt werd met persoonlijke gegevens van de gebruiker. Deze gegevens vallen onder de Privacywetgeving. Zeker nu de nieuwe AVG van kracht is, waarin nieuwe strenge richtlijnen staan voor het verwerken van persoonsgegevens, was het essentieel dat de gegevens van de gebruiker goed afgehandeld en verwerkt werden om zo de privacy en rechten van de gebruiker te waarborgen (Meindersma, 2018).

De doelgroep van het project waren de medewerkers en docenten, samengevoegd ongeveer 4900 personen. De medewerkers en docenten moeten een vettingprocedure ondergaan waarin hun identiteit wordt geverifieerd. Deze procedure zorgt ervoor dat de identiteit van de docenten en werknemers geregistreerd en bewezen zijn, zodat het zeker is dat een account daadwerkelijk gebruikt wordt door de betreffende accounthouder.

[3] https://www.voxweb.nl/nieuws/anonieme-cijfers-studenten-toch-niet-zo-anoniem

1.2 Doelstelling:

De doelstelling van de afstudeeropdracht is om door middel van kwalitatief onderzoek en praktijkvoorbeelden de vettingmethodiek te identificeren die past binnen de organisatorische randvoorwaarden van de Radboud Universiteit en aanbevelingen te geven over hoe het beheer en uitvoering hiervan verantwoord belegd kan worden.

1.3 Probleemstelling:

De Radboud Universiteit wil 2FA implementeren op reguliere applicaties zoals mail, eduvpn en Osiris en belangrijke applicaties zoals beheerservers. Het probleem is dat er nog geen efficiënte manier was om de identiteit van een gebruiker te authentiseren. Daarnaast was het niet helder wat de eisen vanuit het Radboud-bestuur waren en welke wensen de gebruikers hadden over de identiteitscontrole. Aan de hand van de informatie uit de inleiding en in samenwerking met de praktijkcoach was de volgende probleemstelling geformuleerd:

Welke vettingmethodiek past binnen de organisatorische randvoorwaarden van de Radboud Universiteit?

1.4 Onderzoeksvragen:

De probleemstelling wordt door middel van vier onderzoeksvragen beantwoord:

1. *Wat zijn de organisatorische randvoorwaarden voor de vettingmethodiek, van zowel security- als gebruikerskant, van de Radboud Universiteit?*

Het is essentieel voor het onderzoek om een goed duidelijk beeld te hebben van wat de eisen van de Radboud Universiteit zijn voor de vettingmethodiek en het beheer hiervan. De vettingmethodiek moet voldoen aan een aantal securityvoorwaarden om ervoor te zorgen dat de procedure zodanig beveiligd is dat gegevens die de gebruiker deelt beschermd en correct behandeld worden. Daarnaast hanteert de Radboud Universiteit een aantal informatiebeveiligingsnormen en moet er onderzocht worden welke van belang zijn voor de vettingmethodiek. Door middel van een interview moeten de securityvoorwaarden en normen in beeld gebracht worden.

Alleen moet hierbij niet de gebruiker vergeten worden. Het probleem met alleen op de securityvoorwaarden afgaan is dat het proces erg gebruikersonvriendelijk kan worden. Als het proces helemaal waterdicht is door complexe maatregelen maar met tegenzin of niet wordt gebruikt door de gebruiker, heeft het weinig nut. De Radboud Universiteit heeft dit probleem al een aantal keer ondervonden, het meest recente voorbeeld wat de ICT Security Manager noemde is het ‘wachtwoord veranderbeleid’. Het proces om het centrale RU-wachtwoord te veranderen was veel te ingewikkeld geworden omdat het op de diverse apparaten van een gebruiker tegelijkertijd uitgevoerd moest worden. Hierdoor kon het beleid niet gehandhaafd worden. Daarom is het belangrijk om interviews te houden met de werknemers die de voorwaarden van de gebruikers kunnen benoemen. Het proces moet ondanks alle securitymaatregelen wél gebruikersvriendelijk zijn. De security- en gebruikersvoorwaarden vormen de organisatorische randvoorwaarden van de Radboud Universiteit. Deze randvoorwaarden worden gebruikt als een lijst met eisen waarmee de gevonden vettingmethodiek beoordeeld wordt.

2. *Welke normen zijn relevant voor de vettingmethodiek van de Radboud Universiteit?*

Voor de vettingmethodiek is het verstandig om relevante normen, zowel de al gehanteerde normen door de Radboud Universiteit die uit het interview met de Chief Information Security Officer (CISO) komen, als andere nog onbekende normen, te onderzoeken. De normen bevatten voorwaarden die richting geven aan het onderzoek naar de vettingmethodiek. De normen worden daarna als voorwaarde gebruikt om de vettingmethodiek te beoordelen.

3. *Welke van de vettingmethodieken uit het rapport "Remote Vetting for SCSA" scoort het hoogst bij de toetsingscriteria van de Radboud Universiteit?*

Om een volledig beeld te krijgen over welke vettingmethodieken bestaan is het belangrijk om een inventarisatie te doen van de beschikbare vettingmethodieken. Deze methodieken worden geïnventariseerd door gebruik te maken van het rapport "Remote Vetting for SURFconext Strong Authentication". Dit rapport beschrijft en beoordeelt een groot aantal vettingmethodieken die gebruikt worden door verschillende organisaties. Dit is tot nu toe het meest complete en duidelijke rapport over vettingmethodieken. De ICT Security Manager en Project Manager 2FA hebben aangeraden om dit rapport te gebruiken omdat er weinig informatie beschikbaar is over vettingmethodieken. Uit het oogpunt van doelmatigheid is gekozen voor een aanpak waarbij maximaal vier van de hoogst gewaardeerde vettingmethodieken uit het rapport in dit onderzoek te betrekken. De best beoordeelde vettingmethodieken uit het rapport van SURF zijn:

- iDIN;
- DigiD;
- SURFsecureID;
- Idensys;

Daarnaast wordt op verzoek van de praktijkcoach onderzocht of de vettingmethodiek "IRMA" een optie is voor de Radboud Universiteit. IRMA is een applicatie wat ontwikkeld is door de stichting Privacy By Design, wat de gebruiker de mogelijkheid biedt om op een privacy-vriendelijke manier in te loggen. De gebruiker geeft hierbij zelf aan welke persoonsgegevens hij deelt met de organisatie of instelling die om deze gegevens vraagt.

Deze vettingmethodieken worden aan de hand van een aantal toetsingscriteria beoordeeld om te kijken welke methodiek het hoogste scoort en daarmee het meest geschikt is voor de Radboud Universiteit. Deze toetsingscriteria wordt in samenwerking met de Project Manager 2FA opgesteld. Als basis zijn de criteria uit het SURF-rapport gebruikt, die vervolgens door de Project Manager 2FA specifiek zijn gemaakt voor de Radboud Universiteit, zodat daarmee de geschiktheid voor eigen gebruik kan worden getoetst. De best scorende vettingmethodiek wordt dan gebruikt bij de specifieke beoordeling met de organisatorische randvoorwaarden.

4. *Hoe voert het Windesheim de vettingprocedure van hun medewerkers uit en hoe is hun beheer hiervan ingericht?*

Na alle waarnemingen, onderzoeken en gesprekken en voorlopige conclusies die uit de onderzoeksvragen 1 t/m 3 zijn gekomen en op advies van de praktijkcoach, is op zoek gegaan naar een voorbeeld in de praktijk, bij voorkeur een vergelijkbare instelling. Daarmee is een latere invoering bij de Radboud Universiteit gebaat met de ervaringen van die andere instelling. De Hogeschool Windesheim wordt genoemd in het document "Best Practice: Windesheim", omdat zij enige tijd SURFsecureID gebruiken. SURF heeft dit document geschreven. In dit document wordt kort beschreven waarom het Windesheim SURFsecureID heeft gekozen en wordt kort toegelicht hoe zij

hun werknemers hebben geïnformeerd over de nieuwe vettingmethodiek. Door het document is het duidelijk welke vettingmethodiek het Windesheim gebruikt, maar niet hoe de vettingprocedure verloopt binnen de organisatie. Daarom is het belangrijk om met het Windesheim in gesprek te gaan om zo meer informatie te krijgen over waarom zij voor SURFsecureID gekozen en hoe de vettingprocedure ingericht en ingevoerd is. Alleen het onderzoeken hoe de vettingmethodiek gebruikt wordt is niet genoeg, er moet ook gekeken worden naar hoe zij het beheer van deze vettingmethodiek ingericht hebben. Daarnaast kan het Windesheim adviezen geven over hoe de Radboud Universiteit haar werknemers moet informeren over de nieuwe vettingmethodiek.

1.5: Betrokkenen en belanghebbenden:

Bij de betrokken partijen is een onderscheid gemaakt tussen:

- De betrokkenen: deze personen zijn daadwerkelijk betrokken in het uitvoeren van het onderzoek.
- De belanghebbenden: de personen/ afdelingen die belang hebben bij de onderzoeksresultaten. Zij gaan deze resultaten in hun dagelijkse werk invoeren.

De betrokken personen bij het onderzoek zijn weergegeven in tabel 1:

Tabel 1 Betrokkenen

Betrokkenen:	***Waarom?***
ICT Security Manager	Opdrachtgever van het onderzoek. De ICT Security Manager hield zich bezig met het vraagstuk en heeft de opdracht uitbesteed. Daarnaast was hij betrokken bij onderzoeksvraag 1. De informatie uit zijn mail was gebruikt om de securityvoorwaarden op te zetten.
Project Manager 2FA	De Project Manager 2FA was betrokken bij onderzoeksvraag 1 en 3. Hij heeft de informatie over de gebruikersvoorwaarden gegeven. De projectmanager is al een langere tijd bezig om 2FA in te voeren en houdt zich ook bezig met het opstellen van een vettingprocedure.
CISO	De CISO was betrokken bij onderzoeksvraag 1. Hij heeft de securityvoorwaarden aangegeven en de normen benoemd die in onderzoeksvraag 2 onderzocht werden.
Radboud Universiteit Opdrachtgever	De Universiteit heeft de opdracht doorgegeven aan de ICT Security Manager en Project Manager 2FA.
Windesheim te Zwolle	Het Windesheim was geïnterviewd in onderzoeksvraag 4 om erachter te hoe hun vettingprocedure verloopt en hoe zij het beheer hiervan hadden ingericht. Deze instelling heeft gediend als praktijkvoorbeeld en de informatie over hoe zij de vettingmethodiek uitvoeren en beheer hebben ingericht zijn gebruikt om aanbevelingen te maken.

Verder waren er een groot aantal belanghebbenden bij dit project. Belanghebbenden zijn er bij vrijwel elk organisatieonderdeel dat betrokken is bij het toekennen van authenticatiemiddelen en machtigingen en bij de verificatie van de identiteiten bij het toekennen van de machtigingen. Hierbij gaat het zowel om de verantwoordelijke partij (eigenaar), de uitvoerende partij (zie hieronder) en

controlerende partij (auditdienst). Deze partijen hebben een direct belang bij de resultaten van het onderzoek. Ze zijn hieronder beknopt aangegeven. Voor een uitgebreidere uitleg van de belanghebbenden, zie bijlage 2.

De uitvoerende belanghebbenden bij het onderzoek zijn:

- Medewerkers (ICT, balies bij de faculteiten, ICT-servicedesk Universiteitsbibliotheek);
- Studenten;
- Docenten;
- Faculteiten van de Radboud Universiteit;
- Bibliotheken;
- ICT Service Centrum als beheerder van de technologie;

Hoofdstuk 2: Theoretisch kader

In het theoretisch kader worden bestaande literaturen, theorieën en modellen die betrekking hebben op het onderzoek onderzocht, beschreven en verdiept. Door gebruik te maken van een theoretisch kader wordt de betrouwbaarheid en controleerbaarheid van het onderzoek gewaarborgd.

Er zijn veel termen die belangrijk zijn binnen het kader waarin vettingmethodieken zich bevinden. Het is verstandig om de meest algemene termen, die in het onderzoek regelmatig voor zullen komen, te definiëren. Deze termen staan beschreven in de begrippenlijst op pagina 7.

2.1: Wet- en regelgevingen

Tijdens het gehele onderzoek is het noodzakelijk een aantal wet- en regelgevingen aan te houden. Vooral in onderzoeksvraag 1, waarin de organisatorische voorwaarden worden onderzocht, zullen deze wetten en regels terugkomen, ze geven namelijk richting aan het onderzoek en zorgen ervoor dat de vettingmethodiek een aantal kaders heeft en waarin aangegeven staat waar deze rekening mee moet houden. De belangrijkste wet voor dit onderzoek is de Algemene Verordening Gegevensbescherming (AVG). De vettingmethodiek zal namelijk persoonsgegevens van gebruikers opslaan en verwerken. Voor het opslaan en verwerken van persoonsgegevens is momenteel de AVG de belangrijkste wet om aan te voldoen.

Als eerste wordt de AVG toegelicht met de relevante wetsartikelen. Daarna worden de begrippen “compliance” en “privacy by design” uitgelegd.

AVG: Algemene Verordening Gegevensbescherming:

Vanaf 25 mei 2018 is er in de hele Europese Unie een nieuwe privacywetgeving van kracht. De General Data Protection Regulation (GDPR). De GDPR geeft inwoners van de EU meer invloed op wat er met hun privacygevoelige informatie gebeurt en wat bedrijven, overheden en organisaties ermee doen. In Nederland is de GDPR “vertaald” in de AVG. De Radboud Universiteit moet kunnen aantonen dat zij handelen in overeenstemming met de AVG, de Universiteit heeft namelijk een verantwoordingsplicht (ISC, 2018). De AVG heeft een aantal voorwaarden die hieronder kort worden samengevat. De wetsartikelen die een verband met elkaar hebben zijn in het handboek General Data Protection Regulation samengevat zodat het doel van de wetsartikelen helder is. Deze voorwaarden zijn:

- Artikel 5, 6 en 7: Gebruik persoonsgegevens alleen waarvoor ze zijn verzameld.

Voordat men persoonsgegevens gaat verzamelen, moet duidelijk zijn omschreven voor welk doeleinde deze gegevens worden verzameld. Men mag niet voor ieder doel persoonsgegevens verzamelen. De verwerking van persoonsgegevens moet een juridische grondslag hebben.

- Artikel 5 en 25 AVG: Sla niet meer persoonsgegevens op dan nodig.

De persoonsgegevens mogen alleen verzameld en gebruikt worden voor een bepaald doel. Bewaar dus geen extra informatie omdat dat misschien handig is. De persoon in kwestie heeft het recht zijn of haar gegevens in te zien.

- Artikel 6 AVG: Sla persoonsgegevens niet langer op dan nodig.

Bepaal een wettelijk bewaartermijn voor de opgeslagen gegevens. De gegevens mogen niet langer bewaard worden dan noodzakelijk.

- Artikel 5, 24, 32: Sla persoonsgegevens veilig op.

De organisatie moet ervoor zorgen dat er geen onbevoegden bij persoonsgegevens kunnen komen. Versleutel USB-sticks, vermijd gratis clouddiensten als Dropbox en hanteer een clean-desk-policy (BSI, 2018).

- Artikelen 7, 8 en 9: Juistheid van de gegevens en informeren betrokkenen.

Verwerkte gegevens moeten juist zijn en geactualiseerd zijn waar en wanneer nodig. Er moet ook direct gereageerd worden op verzoeken van gerechtigden om inzage, correctie en verwijdering van de gegevens.

Al deze wetsartikelen vormen het uitgangspunt bij het selecteren van de vettingmethodiek voor de Radboud Universiteit. In de vettingmethodiek en bijbehorende procedure worden persoonsgegevens verzameld en de genoemde wetsartikelen geven aan wat de verplichtingen van de Radboud Universiteit naar hun gebruikers toe zijn. De persoonsgegevens die gevraagd worden mogen alleen gebruikt worden om een gebruiker te authentiseren, niet voor andere doeleinden. Daarnaast mogen alleen de persoonsgegevens verzameld worden die nodig zijn voor het specifieke doel en moeten na een bepaalde tijd verwijderd worden. Als laatste moeten deze persoonsgegevens gedurende het gebruik veilig opgeslagen worden op aangewezen servers of diensten en moeten de gebruikers geïnformeerd worden over welke persoonsgegevens opgeslagen worden, waarvoor deze persoonsgegevens gebruikt worden en waar de gebruikers terecht kunnen om inzage in hun gegevens te krijgen.

Privacy by Design:

De vettingmethodiek moet al vanaf het begin maatregelen nemen om de privacy van de gebruikers te waarborgen. Daarom neemt dit onderzoek artikel 25 van de AVG als grondslag: Privacy by Design.

Het bij voorbaat al rekening houden met de privacy van de gebruiker wordt *privacy by design* genoemd. De aandacht voor privacy blijft tijdens de gehele levensduur van het systeem bestaan (Justititia, 2018). Het doel is de beveiliging van persoonsgegevens te optimaliseren (Justititia, 2018). Dat kan al door na te denken over de noodzakelijkheid van het opslaan; welke gegevens zijn nodig en welke niet. Ook moet rekening worden gehouden met de hele levenscyclus van de data: opslag, wijziging en verwijdering (Justititia, 2018).
In de ICT is het tegenwoordig een must om vanaf het begin een systeem goed te ontwerpen in tegenstelling tot het later wijzigen. Aanpassingen achteraf zijn duurder en leveren meestal systemen van mindere kwaliteit (Justititia, 2018).

Compliance:

In de inleiding wordt het volgende genoemd:

“Tijdens het onderzoek was het belangrijk om ervoor te zorgen dat de vettingmethodiek compliant was aan de geldige wet- en regelgevingen en werd vormgegeven conform de normenkaders van de Radboud Universiteit.”

Compliance is een zeer belangrijk principe waar elk bedrijf en organisatie zich mee bezig houdt, zeker na de ingang van de nieuwe AVG. Compliance wordt gedefinieerd als: het naleven van de geldende wetten- en regelgevingen en beleid van de organisatie (University of Adelaide, z.d). De reden waarom het zo’n belangrijk principe is, is dat op non-compliance, het dus niet voldoen aan de wetgeving, behoorlijke sancties staan. Het is dan ook van groot belang dat de vettingmethodiek bij de Radboud Universiteit compliant is aan de geldende wet- en regelgevingen. In onderzoeksvraag 1

wordt onderzocht of er security-normen en algemene normen zijn waaraan de vettingmethodiek moet voldoen.

Om te toetsen of een organisatie werkt en handelt in overeenstemming met de wet- en regelgeving, dient er door een expert een audit uitgevoerd te worden (Bos, 2014). Compliance gaat verder dan het voldoen aan wet- en regelgeving. Volgens het Nederlands Normalisatie Instituut (NEN) hebben organisaties te maken met eisen vanuit stakeholders, opdrachtgevers, brancheverenigingen, bedrijfsregels en gedragscodes[4]. Het NEN adviseert dan ook om te werken met compliance management. Compliance management richt zich op organisaties die moeten voldoen aan de toenemende hoeveelheid en complexiteit van wet- en regelgeving. Aan de hand van compliance management kan dit planmatig worden aangepakt en kan de organisatie zich verantwoorden richting toezichthouders (NEN, 2013). De resultaten uit onderzoeksvraag 1 en 2 geven aan, aan welke regels de vettingmethodiek compliant moet zijn en welke regels van belang zijn bij het beheer van de vettingmethodiek.

2.2: Het spanningsveld tussen privacy en security

In onderzoeksvraag 1 worden de gebruikersvoorwaarden en securityvoorwaarden geïnventariseerd. Tussen deze twee begrippen bestaat een zekere discrepantie. Burgers hechten veel waarde aan hun privacy, maar eisen ook een toename in veiligheid, maar daarvoor is weer meer inzicht nodig in de privacy van de burger (Infosecuritymagazine, 2016).

Privacy en veiligheid zijn beide belangrijke waarden in de hedendaagse samenleving (Blonk, 2017). Het probleem is dat deze waarden onder druk staan: de veiligheid van de samenleving wordt zowel van binnenuit (toenemende polarisatie) als van buitenaf (terrorisme) bedreigd, terwijl het aantasten van de privacy van individuele burgers door toenemende technologische mogelijkheden eenvoudiger dan ooit is (Bron, Kummeling, & Muller, 2007). Zeker door de intrede van 'Big Data', door de digitalisering van de samenleving ontstaat een steeds grotere stroom aan en daarmee gepaard gaande verzameling van gegevens van bijvoorbeeld smartphones, browsers, social networks en van de toenemende toepassing van sensoren in producten en machines die in verbinding staan met het internet (Blonk, 2017). Het gebruik van Big Data veroorzaakt een nieuwe manier van het verzamelen en analyseren van deze gegevens. Het gaat hier niet alleen om de hoeveelheid gegevens, maar bijvoorbeeld ook om het vermogen van software om onverwachte patronen te herkennen (Blonk, 2017). Bij traditionele data-analyse werd vooraf bepaald voor welk doel gegevens werden verzameld en hoe ze zouden worden geanalyseerd, maar met de slimme software van tegenwoordig zijn bedrijven in staat om waardevolle informatie op te halen uit een willekeurige set van gegevens, mits deze groot genoeg is (van Est, Kool, & Timmer, 2015). De gedachte is dat bedrijven en overheidsorganen hun dienstverlening hiermee kunnen verbeteren en zorgen voor meer veiligheid, rechtvaardigheid en maatwerk (Blonk, 2017). Het probleem met Big Data was de onbekendheid bij het publiek wat er met de hoeveelheid data werd gedaan. Er ontstond een spanningsveld tussen de publieke belangen rondom Big Data en individuele belangen van de burger rondom hun privacy (Blonk, 2017). Om dit spanningsveld wat te verminderen is op 25 september 2018 de AVG in werking getreden. Alle bedrijven en organisaties moeten nu duidelijk aangeven wát zij verzamelen en voor welk doeleinde dit wordt gebruikt. Tevens hebben de personen wiens gegevens verzameld worden ten allen tijden toegang tot deze gegevens en het recht op aanvragen van het vernietigen van de gegevens.

[4] https://certificeringsadvies.nl/de-stakeholdersanalyse-iso-9001/

De discussie dat burgers een deel van hun privacy voor veiligheid moeten opgeven is nog steeds een heet hangijzer. Zo liet Europol directeur Rob Wainwright in 2016 tijdens een speech in Den Haag weten:

"*Burgers moeten een deel van hun privacy voor veiligheid opgeven. We erkennen de noodzaak om persoonlijke gegevens te beschermen en het fundamentele recht van privacy op internet. Het groeiende misbruik van legitieme anonimiteit en encryptiediensten en tools voor illegale doeleinden is een serieus probleem voor de opsporing, onderzoek en vervolging, waardoor het een dreiging voor de veiligheid van onze maatschappij wordt. Backdoors, frontdoors, escrow-systemen en het verbieden van encryptie. Het huidige debat hierover en andere mogelijke oplossingen missen het grotere geheel hoe concurrerende vereisten voor veiligheid, privacy en opsporingsdiensten zijn te balanceren. Deze ontwikkelingen houden in dat onze samenleving zich op een kritiek moment bevindt waar een pro-actief en gebalanceerd antwoord noodzakelijk is, waar met alle meningen rekening wordt gehouden."* (Wainwright, 2016)

Vervolgens stelt hij dat privacy en anonimiteit niet als losse rechten moeten worden gezien, maar meer in de context van bredere juridische concepten zoals de vrijheid van meningsuiting. Het is volgens hem de taak van opsporingsdiensten om deze en andere rechten te beschermen.

"Dit is gebaseerd op een sociaal contract, wat inhoudt dat burgers een deel van hun individuele macht afstaan, en binnen duidelijk gedefinieerde en gereguleerde grenzen, een deel van hun privacy in ruil voor veiligheid afstaan." (Wainwright, 2016).

Deze uitspraak lijkt weer in conflict te zijn met artikel 10[5] van de Grondwet, waarin staat dat iedereen recht heeft op eerbiediging van zijn persoonlijke levenssfeer (Blonk, 2017).

Een opvallend gegeven is gebleken dat burgers een tegenstrijdige opvatting hebben over hun privacy. Uit het onderzoeksrapport van Raoul Schildmeijer, Chantal Samson en Harro Koot waarbij een aantal groepssessies zijn gehouden waarin het onderwerp privacy centraal stond, kwam naar voren dat burgers veelal laconiek omgaan met de bescherming van hun persoonsgegevens. Ze klagen over irritante post, mailtjes en dat er veel over hen te vinden is, maar geven anderzijds vrij makkelijk inzage in hun gegevens onder het motto dat ze niets te verbergen hebben (Schildmeijer, Samson, & Koot, 2005). Wat wel een erg interessant gegeven is dat het oordeel uit het kwantitatieve onderzoek veel genuanceerder is dan het oordeel wat uit de groepssessies kwam. In de groep versterkten de deelnemers bij elkaar de opvatting dat *'ze toch al alles van je weten'(de overheid) en 'ze alles van je mogen weten als je niets te verbergen hebt.'* (Schildmeijer, Samson, & Koot, 2005)

Ook in de dagelijkse praktijk is het balanceren tussen enerzijds de bescherming van de privacy en anderzijds de laconieke houding van de burger een probleem. De Radboud Universiteit heeft daarom momenteel moeite om een vettingmethodiek te vinden wat zowel de belangen van de gebruiker als de beveiligingseisen vervuld. De verantwoordelijken voor de beveiliging van de methodiek willen het liefst zo veel als mogelijk persoonlijke attributen van een gebruiker inventariseren om deze zo te authentiseren. De gebruiker wil niet teveel informatie over zichzelf vrijgeven en wil duidelijk weten wat er met deze informatie gebeurt. Daarom moet er een balans worden gevonden tussen de wensen van de security verantwoordelijken en gebruikers.

[5] Artikel 10 Grondwet: Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbieiding van zijn persoonlijke levenssfeer. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt

2.3: Identity Management

Naast dat er met dit onderzoek rekening gehouden moet worden met privacy en security, dient er ook rekening gehouden te worden met identity en access management. Het op te stellen beheer zal toebedeeld kunnen worden aan de Identity Managers van de Radboud Universiteit. Deze beheren reeds alle digitale identiteiten en de daarbij behorende autorisaties. Maar wat is identity management nu eigenlijk?

De vettingmethodiek valt binnen het overkoepelende geheel Identity Management. Identity management houdt zich in de breedste zin bezig met het identificeren van individuen binnen een systeem (Jurg & Valkenburg, 2007). Het hoofddoel van identity management is het controleren of deze individuen daadwerkelijk toegang mogen hebben tot verschillende middelen binnen dit systeem. Dit gebeurt door middel van het associëren van een aantal gedefinieerde gebruikersrechten en beperkingen met de betreffende identiteit (Jurg & Valkenburg, 2007). Met Identity management kan er controle gehouden worden over wie waar toegang tot heeft, de identiteit van een gebruiker wordt namelijk in een netwerk beheerd. Ook gaat het over de vraag of de gebruiker is wie hij zegt dat hij is. De vettingmethodiek valt binnen het overkoepelende geheel Identity Management omdat deze de elektronische identiteitsgegevens van een gebruiker nodig heeft om effectief te kunnen werken. Met elektronische identiteitsgegevens wordt bedoeld: de gegevens die bij een persoon horen en die elektronisch zijn vastgelegd (Jurg & Valkenburg, 2007).

Een aantal belangrijke begrippen binnen identity management zijn authenticatie en autorisatie. Deze twee begrippen zijn van belang voor het onderzoek omdat gebruikers geauthentiseerd en geautoriseerd worden door de vettingmethodiek (Hulsebosch, 2017).

Met authenticatie wordt het proces bedoeld waarmee een persoon zijn identiteit kan aantonen (Jurg & Valkenburg, 2007). Authenticatiemiddelen waarmee de identiteit kan worden aangetoond zijn er in allerlei soorten. Een zwakke vorm van authenticatie is bijvoorbeeld een combinatie wachtwoord/gebruikersnaam (Jurg & Valkenburg, 2007). De sterkste vormen van authenticatie bestaan uit de combinatie van iets wat de gebruiker **weet**, bijvoorbeeld een pincode, en iets wat de gebruiker biometrisch is of **heeft**, bijvoorbeeld een vingerafdruk, irisscan of hardware token (Jurg & Valkenburg, 2007).

Autorisatie is het proces van het verlenen van toegang aan personen of systemen tot de functionaliteit van ICT-diensten (Jurg & Valkenburg, 2007). Idealiter zijn voor autorisatie bedrijfsregels opgesteld waaraan de identiteit van de gebruiker moet voldoen om toegang tot diverse omgevingen te verkrijgen. Bedrijfsregels voor ICT-toegangsautorisatie zijn vaak gebaseerd op de rol (of rollen) die een gebruiker in de organisatie heeft. Om de controle op toegangsrechten voor een verzameling van applicaties te structureren en te beheren, wordt vaak het geldende beveiligingsbeleid en de daaruit voortvloeiende beveiligingsmaatregelen als uitgangspunt genomen. Indien de identity en access-managementoplossingen de beveiligingsmaatregelen volgen, spreekt men van ‘policy based access control’ (Jurg & Valkenburg, 2007). Deze ‘policies’ kunnen diverse uitgangspunten nemen, zoals het onderscheid tussen toegang binnen en buiten het organisatienetwerk, het gebruikte authenticatiemiddel en de functie die een gebruiker in de organisatie vervult. Voorafgaand aan autorisatie is authenticatie nodig, want toegangsrechten kunnen over het algemeen niet precies worden bepaald zonder de identiteit van een persoon te kennen. In sommige gevallen is het echter voldoende om een algemener kenmerk van de gebruiker te kennen, zoals het netwerkadres van zijn werkplek (Jurg & Valkenburg, 2007).

Hoofdstuk 3: Methodologie

In dit hoofdstuk worden de methoden beschreven die gebruikt zijn om de onderzoeksvragen te beantwoorden. In dit hoofdstuk wordt er eerst beschreven of er sprake is van kwantitatief of kwalitatief onderzoek. Dan wordt per onderzoeksvraag de dataverzamelingsmethode, operationalisering (hoe zijn de interviewvragen opgesteld en hoe is de deskresearch uitgevoerd) en data analyse beschreven. Tot slot wordt de validiteit en betrouwbaarheid van het onderzoek verklaard.

3.1 Kwantitatief of kwalitatief onderzoek en dataverzamelingsmethoden:

Er bestaan verschillende manieren om een onderzoek uit te voeren, waaronder een kwantitatief en kwalitatief onderzoek. Bij een kwantitatief onderzoek wordt er gebruik gemaakt van data, getallen of gegevens die gekwantificeerd kunnen worden (Swaen, 2013). Een belangrijk onderscheid tussen kwantitatief en kwalitatief onderzoek is dat er bij kwantitatief onderzoek 'gemeten' wordt en bij kwalitatief niet (Poortinga, 2018). Meten houdt in dit geval in dat er getallen worden toegekend aan objecten of gebeurtenissen. Bij kwantitatief onderzoek gaat het om het verzamelen van kwantificeerbare data. Bij kwalitatief onderzoek is dat niet het geval.
Bij kwalitatief onderzoek wordt niet of nauwelijks gebruik gemaakt van kwantificeerbare data, het onderzoek wordt dan uitgevoerd in de praktijk. De onderzoeker is dan geïnteresseerd in de kennis en meningen over het onderwerp van de onderzochte personen (Verhoeven, 2014).

Om te bepalen of dit onderzoek een kwantitatieve of kwalitatieve aanpak vereist, is er per onderzoeksvraag gekeken welke kwantitatieve of kwalitatieve dataverzamelingsmethoden het beste passen bij de onderzoeksvragen. Om onderzoeksvraag 1, waarbij het duidelijk moet worden wat de security- en gebruikersvoorwaarden voor de vettingmethodiek zijn, en onderzoeksvraag 4, waar er onderzocht is hoe het Windesheim de vettingprocedure uitvoerde en hoe hun beheer is ingericht, zijn interviews gehouden. De interviews waren nodig om de noodzakelijke informatie te achterhalen om deze onderzoeksvragen te beantwoorden. Een interview is een kwalitatieve dataverzamelingsmethode (Verhoeven, 2014).
Onderzoeksvraag 2 is beantwoord door middel van documentanalyse. De benodigde normen moesten gevonden worden tijdens de deskresearch, deze normen waren nog onbekend. Daarna moest de informatie in de gevonden literatuur door middel van documentanalyses gevonden worden. Documentanalyse is een kwalitatieve dataverzamelingsmethode (Verhoeven 2014).
Onderzoeksvraag 3 is ook beantwoord door middel van een documentanalyse. Het rapport "Remote Vetting for SCSA" van SURF was gegeven door de ICT Security Manager om te onderzoeken. In dit rapport zijn verschillende vettingmethodieken beschreven en beoordeeld aan de hand van verschillende criteria.

3.2: Wat zijn de organisatorische randvoorwaarden voor de vettingmethodiek, van zowel security- als gebruikerskant, van de Radboud Universiteit?

Data verzamelingsmethode:

Om zoveel als mogelijk bruikbare informatie omtrent het onderwerp bij de respondenten op te halen was er gebruik gemaakt van een semigestructureerd interview. Volgens Verhoeven (2014) en Baarda (2017) geeft een semigestructureerd interview de mogelijkheid het interview sturing te geven door middel van topics, maar het geeft ook de mogelijkheid om tijdens het interview vragen te stellen die niet van te voren gepland waren als de respondent een interessante opmerking maakte. Zo bleef er een zekere mate van spontaniteit mogelijk tijdens het gesprek. De organisatorische randvoorwaarden waren nergens op papier vastgelegd maar waren wel bekend bij een aantal individuen binnen de Radboud Universiteit. De enige manier om hier achter te komen was door interviews af te nemen om zo de kennis en ervaringen van deze individuen te achterhalen. De gehouden interviews zijn opgenomen zodat de gesprekken later getranscribeerd konden worden. De personen die geïnterviewd zijn worden beschreven in tabel 2.

Tabel 2 Functie geïnterviewde personen en toelichting

Functie	*Toelichting*
Chief Information Security Officer (CISO)	De CISO is verantwoordelijk voor het opstellen van het securitybeleid, toezicht op de naleving en het handhaven ervan bij de Radboud Universiteit. Hij was vanuit zijn functie zeer bekend met de algemene securityvoorwaarden voor de vettingmethodiek.
Project Manager 2FA	De projectmanager van het ISC is al enige tijd bezig om een vettingmethodiek te implementeren. Hij heeft veel overleg gevoerd met de faculteiten van de Radboud Universiteit. Daar heeft hij veel gebruikersvoorwaarden meegekregen en vertelden de verantwoordelijken bij de faculteiten waar de werknemers problemen mee hadden.
ICT Security Manager	De ICT Security Manager heeft veel ervaring met securityvoorwaarden voor processen. De CISO gaf de algemene securityvoorwaarden en de ICT Security Manager kon meer specifieke, praktische securityvoorwaarden geven voor de vettingmethodiek.

Er zijn twee interviews gehouden, namelijk met de CISO en Project Manager 2FA. In de tussentijd was de ICT Security Manager met pensioen gegaan en is hem de vraag gesteld of hij bereid was het volledig uitgewerkte interview met de CISO aan te vullen met zijn input, voor het geval er naar zijn mening nog aspecten ontbraken. De ICT Security Manager was hiertoe bereid en heeft een kort verslag gestuurd waarin hij zijn aanvullingen gaf. Dit verslag zit in bijlage 3.

Dankzij de Project Manager 2FA was er de mogelijkheid om zelf vier weken mee te werken met het vetten van docenten. Dit gaf de mogelijkheid om een participerend observatieonderzoek te houden. Bij een participerende observatie maakt de observator deel uit van de context waarbinnen het gedrag van de mensen bestudeerd wordt (Dingemanse, 2016). Dit vettingmoment voor de docenten gaf de mogelijkheid om te vragen waar de docenten moeite mee hadden.

Operationalisering:

Bij het afnemen van de semi-gestructureerde interviews was er gebruik gemaakt van een vragenlijst waarin de verschillende onderwerpen aan bod kwamen. De security- en gebruikers onderwerpen die genoemd werden in het PvA en de onderwerpen in het theoretisch kader waren als leidraad gebruikt in het opstellen van de vragen:

Security-voorwaarden:

- Wet- en regelgevingen;
- Wensen voor vettingmethodieken;
- De securityvoorwaarden waaraan de vettingmethodiek moet voldoen;
- Gehanteerde normen door de Radboud Universiteit;
- Problemen ondervonden door de Radboud Universiteit;

Gebruikersvoorwaarden:

- Meest voorkomende problemen van de gebruikers;
- Bereidheid van de gebruiker om een proces op te volgen;
- Te ondernemen acties om de vettingmethodiek makkelijk uitvoerbaar voor de gebruiker te maken;

De vragen in deze vragenlijst voor de CISO en Project Manager 2FA waren in samenwerking met de praktijkcoach opgesteld.

Het contact kwam via een persoonlijke benadering tot stand. De CISO en ICT Security Manager hadden in het begin van het onderzoek aangegeven dat zij wilden meehelpen met deze onderzoeksvraag. De Directeur ICT heeft voorgesteld om de Project Manager 2FA te interviewen.

Het interview met de CISO bestond uit 17 vragen. (Bijlage 4) Het interview met de Project Manager 2FA bestond uit 14 vragen. (Bijlage 5)

Na het meewerken aan het vetten de docenten was er gesprek aangegaan met de collega-studenten die hier hadden meegewerkt. Tijdens dit gesprek is gevraagd welke vragen het meest werden gesteld door de docenten. In samenwerking met deze studenten zijn 12 ‘hoofdvragen’ opgesteld.

Data analyse:

Om de data uit het interview te analyseren was er voor gekozen om het interview te transcriberen en te coderen. Door te coderen is de interviewdata op een systematische manier geanalyseerd (Verhoeven, 2014). Er was er voor gekozen om de tekst volledig over te nemen, inclusief alle ‘oh’s’, ‘uhms’, ‘eehm’ en dergelijke, zodat alle informatie die besproken was in het interview op papier terecht kwam.

Daarna was deze tekst gekopieerd in een Excel document. In Excel werden drie tabbladen aangebracht:

1. Originele tekst met alle woorden, pauzes en geluiden erin verwerkt;
2. De aangepaste tekst waarin overbodige woorden, oh’s’, ‘uhms’, ‘eehm’, pauzes en stukken tekst die niets te maken hadden met de eerder genoemde onderwerpen en interviewvragen verwijderd werden;
3. Een tabblad met het axiaal coderingsschema en toelichting;

Om de aangepaste tekst in tabblad 2 te coderen zijn er drie coderingsronden gehouden. De eerste ronde was het open coderen van de stukken tekst. De stukken tekst werden in één of maximaal vijf woorden samengevat om de essentie van het tekstfragment weer te geven (Dingemans, 2017).

Ronde twee was het axiaal coderen van de stukken. Bij het axiaal coderen worden de codes met elkaar vergeleken en worden de bij elkaar horende codes samen binnen een overkoepelende code geplaatst (Dingemans, 2017). De eerder genoemde security- en gebruikersvoorwaarden waren gebruikt om de verschillende hoofdonderwerpen aan te geven. Daarnaast was na het open coderen gekeken of er een aantal onderwerpen binnen deze codes vaker voorkwamen. Deze vaker voorkomende codes zijn samengevoegd tot hun eigen axiaal codes. Het kwam voor dat een aantal tekstfragmenten hetzelfde onderwerp hadden maar met een andere focus. Een voorbeeld hiervan was het kopje “struikelpunten” bij het interview met de CISO. Deze werd opgedeeld in verschillende struikelpunten: onduidelijkheden, technische problemen en menselijke factor. Alle gebruikte axiaal codes met toelichting zijn terug te vinden in bijlage 6.

De axiaal codes werden geplaatst naast de kolom met open codes uit ronde één die overeen kwamen met het onderwerp van de betreffende axiaal code. Zie figuur 1 voor het voorbeeld:

I/R	Tekst	Open Coderen	Axiaal Coderingslaag 1
R	: Ja, de identiteitscontrole wordt voor allerlei dingen he, hier he, (interviewer hoest, twee woorden vallen weg) identiteitscontrole, ophalen van je campuskaart he die wordt gecombineerd met die identiteitscontrole. Ehm, het komt erop neer dat je de juiste rechten bij de juiste persoon ehm wilt hebben, en daardoor wil vaststellen dat als er eeh, middel is wat bij de persoon hoort, dat de persoon dan wel geïdentificeerd is. Nu speelt de recht van inzage van de AVG, we willen ook wel dat diegene die zegt van eeh “doe mij maar alles gegevens” dat dat diegene is van wie de gegevens zijn.	Wens voor vettingmethodiek	Security eisen
R	ook daarvoor hebben we identiteitscontrole		
I	Heeft u er al ervaring mee gehad dat iemand dat wilde?		
R	Ja. Een aantal al. Dus eh, das een hoop werk. En het zijn algemene vragen nog dus. We kunnen niet zeggen van dan moeten we dat systeem hebben en dan hebben we hét antwoord.	Onduidelijk wélke methodiek vettin	Struikelpunt: Onduidelijkheden
I	Dat is dan uiteindelijk wel een goed doel. Een duidelijk doel. Eeeh, weet u ook toevallig welke normen hierbij in acht moeten worden gehouden? Ik heb namelijk zitten zoeken op ISO-normen, kwam ook op een norm van Surf uit.		
R	eehm, Ik heb ook geen normen ofzo die echt voor vetten bedoeld zijn, of voor identiteitscontrole. Maar wel voor eeeehm	Geen specifieke normen voor vettir	Normen: ISO

Figuur 1 Axiaal codering CISO voorbeeld

Ronde drie was het selectief coderen van de axiaal codes. Selectief coderen is het analyseren van de gevonden resultaten in de context van de probleemanalyse (Verhoeven, 2014). Er was een Word document gecreëerd en alle axiaal codes werden daarin geplaatst. Onder deze axiaal codes waren de bijbehorende tekstfragmenten geplaatst. Aan de hand van deze tekstfragmenten was per axiaal code een samenvatting geschreven. Aan het eind van de samenvatting werden alleen axiaal codes die antwoord gaven op de onderzoeksvraag en de uitspraken bewaard die een stuk in de samenvatting extra verklaring of toelichting gaven. De norm die benoemd was in het interview werd gebruikt in onderzoeksvraag 2.

Van de 12 meest voorkomende vragen uit het observatieonderzoek is een Frequently Asked Questions (FAQ) document opgesteld. Deze is te vinden in bijlage 7.

3.3: Welke normen zijn relevant voor de vettingmethodiek van de Radboud Universiteit?

Data verzamelingsmethode:

Om de normen te vinden werd er deskresearch uitgevoerd. Volgens Verhoeven (2014) en van der Zee (2017) wordt deskresearch gebruikt als er gezocht wordt naar bestaande informatie over de onderzoeksvraag door middel van boeken, rapporten en andere informatiebronnen. Door het rapport “Remote Vetting for SCSA”van SURF en het interview met de CISO en waren er een tweetal normen bekend geworden. Om uit te kunnen leggen wat de normen waren en waar de organisatie van de vettingmethodiek zich aan moest houden was het nodig om documenten te vinden die de eisen van de betreffende normen beschreven. Toen de literatuur gevonden was werd er een documentanalyse uitgevoerd. Een documentanalyse het is het analyseren van bestaande documenten (Verhoeven, 2014). De documentanalyse was nodig om de normen te beschrijven.

Uit het interview was één norm naar voren gekomen: de ISO 27001. Om informatie over deze norm te vinden was er gebruik gemaakt van Google Scholar en was de zoekterm “ISO 27001” gebruikt. Het document *“ISO/IEC 27000, 27001 and 27002 for Information Security Management*” viel op omdat het door een groot aantal Google Scholar gebruikers was geciteerd. Na het lezen van de samenvatting van het document was gekozen dit document te gebruiken. Om te controleren of dit document ook over de juiste ISO 27001 ging werd er gecontroleerd aan de hand van de samenvatting op de officiële ISO webpagina of de inhoud overeen kwam. Dit kwam overeen.

In het rapport “Remote Vetting for SCSA” werd de ISO 29115 genoemd. De Levels of Assurance (LoA’s) die worden gebruikt door de Radboud Universiteit komen van SURF. SURF heeft zijn LoA’s gebaseerd op de ISO 29115. Door te googlen op de zoekterm “ISO 29115”, viel het document “ISO/IEC DIS 29115 Information Technology- Security techniques” op. Dit document was erg uitgebreid, in tegenstelling tot alle andere resultaten over de ISO 29115. Om te controleren of dit document ook over de juiste ISO 29115 ging werd ook gecontroleerd aan de hand van de samenvatting op de officiële ISO webpagina of de inhoud overeen kwam. Nadat de samenvatting was gelezen is ervoor gekozen om dit document te gebruiken.

Operationalisering:

Als eerste waren de samenvattingen op de rapporten doorgelezen om te bepalen of deze bruikbaar waren. Tijdens het bestuderen van de documenten werd er al snel de conclusie getrokken dat deze documenten verouderd waren. De officiële webpagina’s van deze normen gaven dat aan. De documenten voor de ISO 27001 en ISO 29115 waren vervangen door nieuwere versies, die niet vrij verkrijgbaar waren. Daarom was ervoor gekozen om niet een diepte-onderzoek te doen, maar om een globale samenvatting te schrijven over de essentie van deze normen. Om de juiste tekst te vinden in de rapporten voor de samenvattingen was er voor gekozen om twee vragen per norm te stellen. Deze antwoorden op de vragen gaven een globaal overzicht van de betreffende norm. De vragen staan in tabel 3.

Tabel 3 Vragen voor de normen:

Norm:	*Te beantwoorden vragen:*
ISO 27001	- Wat is de IS0 27001 ? - Wat zijn de werkzaamheden in de norm?
ISO 29115	- Wat is de ISO 29115 - Hoe worden de LoA’s gedefinieerd?

Data analyse:
Voor de ISO 27001 was hoofdstuk 5 (ISO 27001) uit het rapport samengevat. Dit was gedaan door de tekst te lezen en met een markeerstift de belangrijkste passages aan te geven die de antwoord gaven op de gestelde vragen. Deze passages werden gebruikt om een samenvatting te schrijven.

Bij het document voor de ISO 29115 is er voor gekozen om hoofdstuk 6 (Levels of Assurance) samen te vatten via dezelfde aanpak. Dit hoofdstuk gaf concreet aan wat de betreffende LoA's inhielden en wat de gedachte achter deze niveaus was.

Aan het einde van het onderzoek waren de stukken tekst besproken met een aantal collega's bij het ISC die bekend waren met de onderwerpen om te bespreken of er informatie ontbrak. Aan de hand van hun feedback werd de tekst aangevuld. In samenwerking met de praktijkcoach is bepaald waarom de norm relevant was voor de vettingmethodiek en waar rekening mee gehouden moest worden. De gemarkeerde teksten bleven bewaard in een onderzoeksmap.

3.4: Welke van de vettingmethodieken uit het rapport "Remote Vetting for SCSA" scoort het hoogst bij de toetsingscriteria van de Radboud Universiteit?

Data verzamelingsmethode:
Voor deze onderzoeksvraag was er wederom een documentanalyse nodig. Het rapport "Remote Vetting for SCSA" bevatte veel informatie wat nader bekeken moest worden. Het rapport moest daarom grondig geanalyseerd worden om zo de belangrijkste informatie eruit te halen.

Operationalisering:
Om een goed beeld te geven over de inhoud van de verschillende vettingmethodieken is besloten per vettingmethodiek vier onderdelen te beschrijven:

- Algemene beschrijving van de vettingmethodiek;
- Voorwaarden of nadelen van de vettingmethodiek;
- Verloop van de vettingprocedure van de vettingmethodiek;
- Beoordeling van de vettingmethodiek aan de hand van eigen criteria;

In het SURF-rapport was een criterialijst opgesteld waarmee de vettingmethodieken waren beoordeeld. Deze originele criterialijst is terug te vinden in bijlage 8. In overleg en samenwerking met de Project Manager 2FA werden de SURF-criteria zodanig specifiek gemaakt dat ze daardoor meer van toepassing waren voor de Radboud Universiteit.

Data analyse:
Vanwege de grote hoeveelheid informatie was ervoor gekozen om het onderzoek in een drie fases op te delen. De eerste fase was gebruikt om erachter te komen welke vettingmethodieken verder onderzocht moesten worden. De tweede fase werd gebruikt om per vettingmethodiek een omschrijving te geven over wat de vettingmethodiek is, wat de voordelen en nadelen zijn. In de laatste fase werden de vettingmethodieken door de toetsingscriteria beoordeeld. In de volgende fasebeschrijvingen staan de werkzaamheden die zijn uitgevoerd.

Fase 1: Verkennen vettingmethodieken

In deze fase waren de hoogst scorende vettingmethodieken uit het SURF-rapport nader bekeken. In figuur 2 zijn de vettingmethodieken weergegeven. De cijfers en kleuren in de vakken geven de score aan. Rood is één punt, geel is drie punten en groen is 5 punten. Er was in overleg met de Project Manager 2FA voor gekozen om uit het oogpunt van doelmatigheid alleen de methodieken uit te kiezen die boven de 35 punten scoorden. De cijfers in de gekleurde vakken gaven de scores aan. Hoe

hoger het cijfer, hoe beter het onderdeel scoorde. De methodieken die meer dan 35 punten scoorden zijn besproken met de Project Manager 2FA. Deze had daarna aangegeven dat video, app optical en NFC niet geschikt waren voor de Radboud Universiteit. De gekozen vettingmethodieken waren: iDIN, Idensys, DigiD en SURFsecureID. Idensys en DigiD vallen beide onder kopje 'derived eIDAS' in de tabel. De Project Manager 2FA gaf ook aan dat er onderzocht kon worden of de vettingmethodiek IRMA een optie was voor de Radboud Universiteit.

Requirement	Door	Video	App Optical	App NFC	Derived iDIN	Derived eIDAS	Central desk	Reuse desk	Com. based
Easy to use by user	5	5	5	5	5	5	1	3	5
Easy to organize by institution	5	5	5	5	5	5	3	3	1
Limited impact on SCSA service	1	1	3	3	3	3	5	3	5
Straight-through processing	3	3	3	5	5	5	3	3	3
High coverage / penetration rate	1	5	5	3	3	1	1	3	5
LoA 2/Low or 3/Subst.	3	3	3	5	3	3	5	3	1
Costs	3	3	3	3	5	5	5	3	3
Controllability / auditability	5	5	5	5	5	5	5	3	1
Future proof & maturity	5	3	3	5	5	3	5	3	1
Total score	**31**	**33**	**35**	**39**	**39**	**35**	**33**	**27**	**25**

Figuur 2 SURF score kaart vettingmethodieken

Fase 2: Omschrijving vettingmethodiek en procedure met nadelen:

In deze fase was er per gevonden vettingmethodiek een omschrijving gegeven met daarin algemene informatie over de methodiek, hoe de vettingprocedure binnen de methodiek verloopt en wat de nadelen waren. Om de juiste omschrijvingen te geven waren de webpagina's van de officiële ontwikkelaars van de vettingmethodieken opgezocht. Deze werden gevonden door de naam van de vettingmethodiek op Google in te vullen. Alle correcte webpagina's stonden binnen de eerste drie resultaten. De nadelen werden uit het SURF-rapport gehaald, deze waren per vettingmethodiek concreet beschreven. Daarna was er per vettingmethodiek de vettingprocedure uitgeschreven die in het SURF-rapport stond. De beschrijvingen van de vettingprocedures waren niet zo uitgebreid op de webpagina's weergegeven, daarom was ervoor gekozen om deze uit het SURF-rapport te halen.

Fase 3: Beoordeling vettingmethodiek met toetsingscriteria:

In de laatste fase werden de vettingmethodieken aan de hand van toetsingscriteria van de Radboud Universiteit gewaardeerd. In de tabellen worden de voor- en nadelen aangegeven van de vettingmethodiek. De beoordelingen van de criteria waren uiteindelijk beoordeeld met de kleuren groen, oranje en rood. In tabel 4 staat de uitleg van deze kleuren. De toetsingscriteria van de Radboud Universiteit is weergegeven in bijlage 9.

Tabel 4 Scorelijst verklaring

Groen:	Voldoende.
Oranje	Twijfelachtig: Er zijn positieve punten te benoemen maar ook negatieve punten.
Rood	Onvoldoende.

3.5: Hoe voert het Windesheim de vettingprocedure van hun medewerkers uit en hoe is hun beheer hiervan ingericht?

Data verzamelingsmethode:

In het “Remote Vetting for SCSA” rapport van SURF was een instelling gevonden die als ‘Best Practice” werd bestempeld. Deze instelling was de Hogeschool Windesheim. Er was contact opgenomen met een vertegenwoordiger van SURF en deze had de contactgegevens gegeven van de projectmanager bij het Windesheim. Er was contact met de projectmanager opgenomen en deze was enthousiast om te helpen. Tevens nam hij iemand van de servicebalie mee naar het gesprek. Het gesprek werd, met goedkeuring van de respondenten, opgenomen.

Om zoveel als mogelijk bruikbare informatie omtrent het onderwerp uit de respondenten te krijgen was er weer gebruik gemaakt van een semi-gestructureerd interview.. De reden waarom er voor een semi-gestructureerd interview was gekozen was omdat er achterhaald moest worden hoe de respondent zijn vettingprocedure had opgesteld en het beheer hiervan had ingericht. Daarnaast moest er achterhaald worden waarom het Windesheim voor de desbetreffende procedure en inrichting had gekozen. Deze informatie was niet vrij beschikbaar en moest door middel van een interview achterhaald worden. Tevens kon er bij dit interview gevraagd worden naar adviezen van de collega-instelling voor de Radboud Universiteit om het vettingprocedure succesvol te implementeren binnen de organisatie en haar gebruikers.

Het interview bestond uit acht vragen. Deze zijn terug te vinden in bijlage 10.

Operationalisering:

Om de vragen voor het Windesheim op te stellen waren onderwerpen gebruikt die gerelateerd aan de onderzoeksvraag zijn:

- Het gebruikte vettingmethodiek van de instelling;
- De werking van het proces;
- Hoe het proces is opgesteld;
- Hoe het beheer van het benoemde proces is ingedeeld;
- Adviezen voor de Radboud Universiteit;

De resultaten bij deze onderwerpen konden de onderzoeksvraag beantwoorden.

Daarnaast was het document “Best Practice: Windesheim” gelezen. Alle interessante observaties werden aangestreept. Deze observaties waren meegenomen in het opstellen van de vragen voor het interview.

De opgestelde vragen waren naar de praktijkcoach en Project Manager opgestuurd voor controle en feedback. De goedgekeurde lijst werd een week voordat het interview zou plaatsvinden gestuurd naar de respondent zodat hij zich kon voorbereiden.

Data analyse:

Om de data te analyseren uit het interview was er voor gekozen om exact dezelfde data analyse methodiek te gebruiken als bij onderzoeksvraag 1, namelijk door het interview te transcriberen en coderen. De gebruikte axiaal codes zijn terug te vinden in bijlage 11.

3.6: Betrouwbaarheid en validiteit

De betrouwbaarheid van onderzoeksresultaten geeft aan in hoeverre het onderzoek vrij is van toevallige fouten. Om de betrouwbaarheid voldoende te kunnen testen moet een onderzoek herhaalbaar zijn (Verhoeven, 2014). Validiteit bepaald in welke mate de resultaten uit het onderzoek kloppen met de werkelijkheid (Swaen, 2014).

De betrouwbaarheid en validiteit van onderzoeksvragen 1 en 4 zijn gewaarborgd door de interviews op te nemen (Dingemanse, 2017; Verhoeven, 2014) Dit is vooraf in de mail met de respondent afgestemd, zodat de toestemming ook vastgelegd was. Het opnemen van de interviews hebben ervoor gezorgd dat het transcriberen van de interviews veel efficiënter verliep omdat de interviews teruggeluisterd konden worden. Na het transcriberen zijn de teksten opgestuurd naar de respondenten met de vraag of zij het eens waren met de genoteerde teksten. Als zij het hier niet mee eens waren werd de tekst aan de hand van hun feedback veranderd. Hierdoor wordt de kans op misinterpretaties verkleind. Daarnaast geeft het ook de inhoud meer validiteit omdat zowel de interviewer en respondent inzage hebben in het stuk en de fouten eruit kunnen halen (Verhoeven, 2014).

De betrouwbaarheid en validiteit van onderzoeksvraag 2 is gewaarborgd door alleen hooggewaardeerde documenten te gebruiken die via Google Scholar zijn gevonden. De gevonden documenten hadden een groot aantal gebruikers die het stuk citeerden in hun eigen onderzoek. Daarnaast zijn deze documenten gepubliceerd door bekende internationale universiteiten en mag er van uit worden gegaan dat deze objectief geschreven zijn. Om de betrouwbaarheid en validiteit van het onderzoeksproces van onderzoeksvraag 2 te waarborgen is er een audit trail bijgehouden. Volgens Swaen (2016) is een audit trail een beschrijving van het onderzoeksproces. De gebruikte zoektermen en ondernomen werkzaamheden tijdens het proces om de normen te vinden zijn vastgelegd in een logboek zodat het onderzoek eventueel herhaald kan worden. Daarnaast zijn de resultaten opgestuurd naar de CISO om te controleren of de informatie klopte en van toepassing was voor de Radboud Universiteit.

Om de betrouwbaarheid en validiteit van onderzoeksvraag 3 te waarborgen is enkel gebruik gemaakt van de informatie in het rapport van SURF en de desbetreffende ontwikkelaars van de vettingmethodieken. Er is een audit trail bijgehouden over hoe de data-analyse van de gegevens is gedaan en over hoe de webpagina's van de ontwikkelaars gevonden zijn. De toetsingscriteria zijn in samenwerking met de Project Manager 2FA opgesteld. Daarnaast zijn de uiteindelijke resultaten en conclusies naar de Project Manager 2FA gestuurd voor controle en eventuele feedback.

Het oorspronkelijke plan bij onderzoeksvraag 4 was dat er meerdere instellingen en organisaties geïnterviewd zouden worden. Helaas was er maar één instelling die een bijdrage kon leveren. Er is ervoor gekozen om dit interview toch op te nemen in de scriptie, want het interview gaf waardevolle informatie over SURFsecureID. De manier waarom het Windesheim SURFsecureID gebruikt en hoe hun beheer hiervan is door SURF benoemd tot 'Best Practice'. Het Windesheim kon daarom adviezen geven over hoe de Radboud Universiteit de vettingmethodiek succesvol kan implementeren en hoe de medewerkers geïnformeerd en begeleid kunnen worden.

Hoofdstuk 4: Resultaten

In dit hoofdstuk worden de resultaten per onderzoeksvraag weergegeven die uit het onderzoek naar voren zijn gekomen.

4.1 Onderzoeksvraag 1

Wat zijn de organisatorische randvoorwaarden voor de vettingmethodiek, van zowel Security- als gebruikerskant, van de Radboud Universiteit?

In deze onderzoeksvraag is er door middel van twee semi-gestructureerde interviews onderzocht wat de organisatorische randvoorwaarden voor de vettingmethodiek zijn. De resultaten van de indicatoren voor de security- en gebruikersvoorwaarden uit het onderzoek worden eerst kort weergegeven in tabel 5 en 6. Daarna volgt per indicator de volledige uitleg met quotes uit het interview.

De 'CISO' in de quotes bij de securityvoorwaarden duidt de Chief Information Security Officer aan. De 'PM' in de quotes bij de gebruikersvoorwaarden duidt de Project Manager aan.

4.1.1 Securityvoorwaarden

Tabel 5 Indicatoren securityvoorwaarden

Indicator	*Resultaat:*
Securityvoorwaarden waaraan de vettingmethodiek moet voldoen:	Zie kopje security eisen op pagina 29 & 30.
Belangrijke normen:	ISO 27001.
Wet- en regelgeving:	Algemene Verordening Gegevensbescherming (AVG), cookiewet, portret- en auteursrechten.
Problemen ondervonden door de Radboud Universiteit:	De ISO 27001 en AVG bevatten erg veel tekst, zonder concrete aanbevelingen over hoe een proces moet worden ingericht en waar het precies aan moet voldoen. Daarnaast heeft de Radboud Universiteit een complexe cultuur, de faculteiten hebben de neiging "orders" van hogerhand (CvB) niet direct te aanvaarden.
Wensen voor vettingmethodiek	IRMA als vettingmethodiek (hoofdstuk 4.3.5)

Securityvoorwaarden waaraan de vettingmethodiek moet voldoen:

CISO: "het komt erop neer dat je de juiste rechten bij de juiste persoon wilt hebben, en daardoor wil vaststellen dat als er eeh, middel is wat bij de persoon hoort, dat de persoon dan wel geïdentificeerd is. Nu speelt het recht van inzage van de AVG, we willen ook wel dat diegene die zegt van "doe mij maar alle gegevens" dat dat diegene is van wie de gegevens zijn."

De securityvoorwaarden die in het interview naar voren komen zijn:

- Zekerheid dat de persoon die een token krijgt, ook daadwerkelijk die persoon is;
- De vettingprocedure past binnen de regels van de ISO 27001;
- Verbetering terugname apparatuur van werknemers. Werklaptops en werktelefoons moeten geregistreerd zijn zodat bekend is wie welk apparaat in gebruik had;
- Waarborging recht van inzage in de persoonsgegevens van een persoon;
- Noodzakelijke wetten worden gevolgd;

De voorwaarden uit de mail van de ICT Security Manager (bijlage 3) zijn als volgt:

1. Indien bij de vetting fysieke toegangsmiddelen zoals yubikeys verstrekt worden, zijn deze middelen beschermd opgeslagen geweest. Toegang tot deze opslag is beperkt tot geautoriseerde personen en wordt gemonitord en is traceerbaar.
2. Bij de uitreiking van toegangsmiddelen wordt de vetting uitgevoerd door overlegging van een wettelijk geldend identiteitsbewijs. Hierbij wordt vastgelegd wat noodzakelijk is voor de auditeerbaarheid.
3. Er is een procedure voor het innemen van toegekende toegangsmiddelen en de registratie hiervan.
4. Er is een mogelijkheid toegekende toegangsmiddelen op afstand ongeldig te maken.
5. De geldigheid van toegangsmiddelen is in tijd beperkt.

Belangrijke normen:

CISO: "Ehm ja de ISO 27001 is een leidraad, ehm, samen met de NCSC.. eehm, Ik heb ook geen normen ofzo die echt voor vetten bedoeld zijn, of voor identiteitscontrole.""

De belangrijkste norm die benoemd wordt in het interview is de ISO 27001. De uitleg van ISO 27001 zelf is vrij onduidelijk en globaal. Er zijn op dit moment geen concrete normen voor twee-factor-authenticatie en vettingprocedures volgens de CISO.

Wet- en regelgeving:

CISO: "Naja als er een website voor opgericht is, met cookies, dan zit dat ook onder de cookiewet. Er worden hopelijk geen foto's genomen want dan krijg je ook nog portret- en auteursrechten. Da's met beeldmateriaal een probleem, dat daar vaak wetten meespelen, dus portretrecht van de fotograaf, auteursrecht,"

Uit het interview zijn een aantal belangrijke wetten naar voren gekomen. Als eerste is er de AVG. Hier moet de vettingmethodiek aan voldoen. De belangrijkste wetsartikelen zijn al eerder benoemd in het theoretisch kader en deze zijn bevestigd door de CISO. Daarnaast noemde de CISO een aantal andere wetten waarmee rekening moet worden gehouden:

- *Cookiewet:*

Als er gebruik gemaakt wordt van een website, zal er ook gebruik worden gemaakt van cookies. Door de cookiewet zal de webpagina verplicht moeten vermelden dat er gebruik wordt gemaakt van cookies.

- *Portret- en auteursrechten.*

Als er gebruik wordt gemaakt van foto's voor bijvoorbeeld werknemerspasjes, zal men te maken krijgen met de portret- en auteursrechten. Dit houdt in dat diegene van wie de foto is volledige controle heeft over zijn/haar foto's en wat daar mee gebeurt.

Problemen ondervonden door de Radboud Universiteit:

CISO: "Wat ik al zei over die ISO 27001 geldt ook voor de AVG, er staat heel veel tekst in, als je vraagt van wat moet ik nou doen, nou dan krijg je een hoop risico's te horen en een hoop waar je rekening mee moet houden maar wat je nou echt moet doen staat er niet in. En hoe je het moet doen ook niet. Dus das wel een algemeen probleem met die verordening."

De CISO gaf aan dat er een aantal onduidelijkheden zijn voor de Radboud Universiteit. De ISO 27001 en AVG bevatten erg veel tekst, zonder concrete aanbevelingen over hoe een proces moet worden ingericht en waar het precies aan moet voldoen. Dat moet bepaald worden door diegene die het proces opstelt. Waar men ook tegen aan loopt is dat als er gevraagd wordt: 'wat moet er worden gedaan om aan de AVG te voldoen?' er eerder wordt verteld welke risico's er zijn dan concrete plannen om te voldoen aan de eisen.

CISO:" ja naja dat is cultuur he, ze proberen iets tegen te houden wat ze eigenlijk in het dagelijkse leven wel zullen doen maar he ."

Daarnaast is een opvallend gegeven uit het interview dat de cultuur binnen de Radboud Universiteit wordt benoemd. Er wordt weinig meegewerkt door de werknemers binnen de faculteit terwijl het een handeling betreft die al vaak in het dagelijkse leven wordt uitgevoerd. Bijvoorbeeld voor bankzaken gebruikt men privé wel degelijk een vorm van 2FA.

Suggesties voor vettingmethodiek:

CISO: " het IRMA idee is dat de gebruiker dat die control heeft over zijn gegevens maar dat je dus wel een enorme zekerheid aan die gebruiker kan vragen op het moment dat het nodig is."

In het interview wordt IRMA genoemd. Een van de grote voordelen van IRMA volgens de CISO is dat het de mogelijkheid biedt aan de gebruiker om volledige controle over zijn eigen identiteit te hebben. IRMA stelt de gebruiker in staat om zelf aan te geven welke gegevens hij wil vrijgeven.

4.1.2 Gebruikersvoorwaarden

Tabel 6 Indicatoren gebruikersvoorwaarden

Indicator:	*Resultaat:*
Meest voorkomende problemen van de gebruikers:	Geen tijd, moeite en onbegrip voor 2FA en vettingprocedures.
Bereidheid van de gebruiker om een vettingprocedure te volgen	Lastige organisatiestructuur en cultuur zorgen ervoor dat 2FA moeilijk geïmplementeerd wordt. Medewerkers en faculteiten verzetten zich tegen de vettingprocedures omdat het als tijdrovend wordt gezien.
Te ondernemen acties om de vettingmethodiek makkelijk uitvoerbaar voor de gebruiker te maken:	LoA 2 en 3 worden gebruikt. Er is een wens om Microsoft ADFS te gebruiken om 2FA makkelijker te implementeren.

Meest voorkomende problemen van de gebruikers:

Door het interview is het duidelijk geworden dat de gebruikers op de Radboud Universiteit een aantal bezwaren hebben tegen het uitvoeren van een vettingprocedure. Deze bezwaren zijn onder te verdelen in de volgende categorieën:

- *Tijd:*

PM: "Ze moeten tijd vrijmaken in hun, naar hun zeggen overvolle agenda, men zegt daar allemaal geen tijd voor te hebben. Men moet dan ook nog langs een balie, zijn ze ook weer tijd voor kwijt en dan moeten ze iets nieuws aanleren. Dat vinden ze heel vervelend"

Om een werknemer te vetten zal er een procedure doorlopen moeten worden. Deze procedure zal tijd innemen. Tijd wat vele docenten, naar hun mening, niet hebben in hun overvolle agenda's. De docenten moeten dan tijd vrijmaken om de mail met de mededeling te lezen, de handeling uit te voeren, langs een informatiepunt te gaan en de procedure daar af te maken.

- *Moeite:*

PM: "*Ja, vooral de oudere generatie eeh, is onbekend met het gebruik van smartphones. Of soms hebben ze er al maar kunnen ze er niet écht goed mee omgaan. Dat is wel een punt, ik denk dat die, dat dat is ook om denk ik omdat zij minder gewend zijn om smartphones te gebruiken maar.. ja er zit ook iets van een kritische houding, die overigens terecht is ten aanzien van diensten als Google en Apple.*

De handelingen die de docenten moeten uitvoeren worden als grote last ervaren. Uit het interview en eigen ervaring is gebleken dat veel docenten moeite hebben om de aanwijzingen te volgen in de notificatiemail en snappen ze niet waarom 2FA gebruikt wordt. Daarnaast wordt er veel moeite ondervonden door de oudere docenten met de smartphones. Uit het interview wordt het duidelijk dat de oudere generatie meer moeite heeft met smartphones en elektronica aangezien zij er niet mee opgegroeid zijn. De jongere docenten hebben minder moeite om de procedure te volgen.

- *Onbegrip:*

Een van de meest veel voorkomende vragen uit de FAQ is: 'Waarom moeten we dit doen?'. Docenten weten niet waarom zij zich moeten laten vetten. Tevens zijn er een aantal docenten die weerstand

bieden tegen het feit dat er nu een app gedownload moet worden op hun telefoon. Zij vertrouwen de diensten van Apple en Google niet, wat terecht is.

Bereidheid van de gebruiker om een vettingprocedure te volgen:

PM: “de ˜Radboud Universiteit is een organisatie die niet een strakke bestuurshiërarchie heeft, we zitten in de academische wereld en daarin is men gewend om alles, tot elke punt en elke komma ter discussie te stellen, daar een mening over te hebben. Je mag wel kritisch zijn maar op een gegeven moment moet je het ook accepteren dat er dingen ingevoerd worden en nu is het zo dat elke faculteit denkt "ja ho eens even, dat zullen wij nog wel eens zien of wij dat gaan doen want daar hebben wij echt geen tijd voor, kost geld en kost tijd, ehm, dat bepalen wij zelf wel." En nou, bij universiteiten en specifiek bij de Radboud Universiteit is mijn.. ja, wil men dat zelf bepalen.”

De bereidheid om een vettingprocedure te volgen verschilt per werknemer, daar kan geen concreet antwoord op worden gegeven. Het is wel duidelijk geworden dat de faculteiten van de Radboud Universiteit bekend staan om hun kritische houding en dat dit heeft geleid tot weerstand tegen 2FA en de te volgen vettingprocedure binnen de faculteiten. De Radboud Universiteit bestaat uit zeven faculteiten die zelf de dagelijkse werkzaamheden bepalen. Deze faculteiten hebben allemaal een academische houding, wat wil zeggen: een zeer kritische denkwijze. Veel besluiten van het CvB worden vaak ontvangen met deze kritische houding. Wat aan de ene kant erg goed is, besluiten worden niet lukraak aangenomen of uitgevoerd en worden veelal goed beoordeeld. Maar aan de andere kant betekent het ook dat besluiten die genomen worden voor de veiligheid van de werknemers, data en bedrijfsprocessen kritisch onthaald en slecht gehandhaafd worden als de faculteiten het niet eens zijn met deze besluiten.

Te ondernemen acties om de vettingmethodiek makkelijk uitvoerbaar voor de gebruiker te maken:

PM: “Ja. Eigenlijk willen we... Kijk, wij hanteren de methodiek van Surf, die heeft drie niveaus. Je hebt LOA 1, username password. Eh, LOA 2 is software token en LOA 3 is Yubikey, het hardware token. Eigenlijk willen we voor de meest kritische toepassingen LOA 3 hebben.”

PM: “ADFS... Dus dat is eigenlijk het platform waar je eigenlijk alles onder kunt hangen. Dat is voor de gebruiker prettig, dat ie maar één kent, dat ie niet voor elke dienst een nieuwe moet leren. Hij heeft één keer de werkwijze van een software token, IRMA of een andere app, heeft ie geleerd”

PM: “als je bijvoorbeeld iets als ADFS ingericht hebt, dan kun je, dan heb je één aansluitpunt voor die tweefactor dienst, dan is het veel gemakkelijker om bijvoorbeeld de Office365 diensten om die voor allemaal of een enkele, per dienst te gaan bepalen. Deze dienst willen wij twee factor authenticatie geven, bijvoorbeeld email, dat is een hele voor de hand liggende, om daar het voor in te voeren. Daar kun je echt gewoon vinkjes neerzetten, dan is de uitrol eeh, is is eh, zowel technisch als organisatorisch veel eenvoudiger.”

In het interview zijn een paar acties aangegeven die uitgevoerd moeten worden. De eerste is dat LoA 2 voor reguliere applicaties en LoA 3 voor belangrijke applicaties gebruikt moet worden. Daarnaast wordt het duidelijk dat ADFS een zeer behulpzaam middel is voor het integreren van 2FA. ADFS is een systeem wat het makkelijk maakt om 2FA te binden aan applicaties.

4.2: Onderzoeksvraag 2:

Welke normen zijn relevant voor de vettingmethodiek van de Radboud Universiteit?

De belangrijkste informatie over de normen zijn door middel van een documentanalyse uit de documenten “ISO/IEC DIS 29115 Information Technology- Security techniques”, “ISO/IEC 27000, 27001 and 27002 for Information Security management”” gehaald en zijn hieronder samengevat.

4.2.1: ISO 27001

ISO 27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. De Radboud Universiteit hanteert al enige tijd de ISO 27001. Met de ISO 27001 certificering laat de Radboud Universiteit zien dat hun Informatie Security Management Systeem (ISMS) voldoet aan de eisen rondom informatiebeveiliging. Het is belangrijk dat de vettingmethodiek meegenomen wordt in de periodieke uitvoering van de risicoanalyse & -beoordeling, waarmee specifieke organisatierisico’s rond informatiebeveiliging worden weggenomen door passende beveiligingsmaatregelen.

De ISO 27001 is in 2005 onder de titel “Information technology- Security Techniques- Information security management systems –Requirements” gepubliceerd (Disterer, 2013). Het beschrijft in 42 pagina’s de eisen waaraan het ISMS aan moet voldoen om het certificaat te halen. Concrete aanbevelingen om deze eisen te vervullen worden niet gegeven door de standaard, het bedrijf moet deze maatregelen zelf ontwikkelen en implementeren, aangezien elke organisatie anders is. De focus van ISO 27001 is gericht op het plannen, implementeren, functioneren en continue monitoring en verbetering van een proces georiënteerd ISMS (Disterer, 2013). De scope van een ISMS moet gedefinieerd worden tijdens de planning en implementatie fase. Risico’s moeten worden geïdentificeerd en beoordeeld worden op hun kans en impact. Vervolgens moeten er maatregelen worden bedacht om de impact van de risico’s aan te pakken. Adequate training moet worden ontwikkeld om de procedures te implementeren en awareness te genereren. De compliance van de procedures moeten continu gemonitord worden. De getroffen maatregelen moeten tevens continu gemonitord worden zodat er steeds verbeteringen aangebracht kunnen worden.

4.2.2 ISO 29115

In het onderzoek is de term LoA, oftewel “Level of Assurance”, al meerdere malen voorbij gekomen. De Radboud Universiteit wil gebruikmaken van LoA 2 voor reguliere applicaties en LoA 3 voor belangrijke applicaties . Hoewel deze norm niet zozeer noodzakelijk voor de Radboud Universiteit om daadwerkelijk op te nemen in de bedrijfsprocessen, is het wel belangrijk om op de hoogte te zijn van deze norm en welke eisen deze LoA’s hebben volgens de norm. De risicotabel kan meegenomen worden tijdens toekomstige risicoanalyses om de LoA’s van applicaties te bepalen.

De norm waarin de LoA’s expliciet worden benoemd is de ISO 29115. De ISO 29115 geeft vier niveaus aan LoA’s voor entiteit (gebruiker in dit geval) authenticatie. Elke LoA beschrijft de mate van hoe betrouwbaar het identificatieproces moet zijn, zodat het zeker is dat de entiteit ook daadwerkelijk de daaraan verbonden identiteit heeft.
LoA 1 is het laagste Level of Assurance en LoA 4 is het hoogste Level of Assurance. Het bepalen van de LoA hangt af van de gegeven situatie en de bijbehorende factoren. Het bepalen van de vereiste LoA is gebaseerd op risico’s: de consequenties van een authenticatiefout en/of het misbruik van de inloggegevens van de gebruiker hebben een bepaalde impact en een grote kans dat het kan gebeuren. LoA’s worden gebruikt voor hogere risico’s. De volledige toelichting van de verschillende LoA’s is terug te vinden in bijlage 12.

De selectie van de gepaste LoA moet gebaseerd zijn op een risicoanalyse die gemaakt is van de interne applicaties die een login vereisen. Een voorbeeld van een risicotabel uit de ISO 29115 is weergegeven in figuur 3:

Potential impact of authentication errors	Level of assurance*			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Min	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to the entity, its programs, or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Mod	Sub	High
Personal safety	N/A	N/A	Min Mod	Sub High
Civil or criminal violations	N/A	Min	Sub	High
* Min=Minimum; Mod=Moderate; Sub=Substantial; High=High				

Figuur 3 Risicotabel ISO29115

In deze tabel wordt de potentiële impact van een authenticatie error (misbruik van de identiteit van een gebruiker) aangegeven door de Level of Assurance. Hoe lager de Level of Assurance, hoe minder groot de impact van een risico is. Dit houdt in dat de impact van de risico's bij zaken die bijvoorbeeld LoA 1 gebruiken minimaal of zelfs helemaal niet aanwezig zijn.

4.3 Onderzoeksvraag 3:

Welke van de vettingmethodieken uit het rapport "Remote Vetting for SCSA" scoort het hoogst bij de toetsingscriteria van de Radboud Universiteit?

In deze onderzoeksvraag is door middel van een documentanalyse onderzocht welke vettingmethodiek het hoogste scoort bij de toetsingscriteria van de Radboud Universiteit. Als eerste wordt er een algemene omschrijving gegeven over de vettingmethodiek, daarna worden de voorwaarden en nadelen van de vettingmethodieken benoemd. De te doorlopen stappen per vettingmethodiek zijn beschreven in bijlage 13. Als laatste is een tabel geplaatst met daarin de beoordelingen die de vettingmethodieken hebben gekregen aan de hand van de toetsingscriteria. De volledige uitwerking van de beoordelingen per vettingmethodiek is terug te vinden in bijlage 14.

4.3.1: SURFsecureID

De SURFsecureID methodiek is een manier om fysiek de identiteit van de gebruiker te controleren aangezien deze zich moet melden bij een servicebalie. Voor de organisatie is dit een van de veiligste manieren om zekerheid te krijgen over de identiteit van een gebruiker. De persoon heeft zich fysiek moeten melden en het persoonsbewijs is bekeken en gecontroleerd. Met SURFsecureID is het mogelijk om zowel LoA 2 als LoA 3 te gebruiken. Bij LoA 2 wordt gebruik gemaakt van de app Tiqr. Bij LoA wordt er gebruik gemaakt van een Yubikey. SURFsecureID noteert alleen de naam, het werknummer, e-mailadres en de laatste twee tekens van een identiteitsbewijs. Om SURFsecureID te gebruiken zijn er Registration Authorities (RA's) en Registration Authority Administrators (RAA's) nodig. De RA is bevoegd om werknemers te authentiseren. De RAA benoemt deze RA's.

Het nadeel van SURFsecureID is dat dit fysiek moet gebeuren. De Radboud Universiteit is van plan om zich te richten op remote vetting, wat betekent: vetting op afstand. De gebruiker hoeft dan niet fysiek langs te komen bij een balie, maar kan zich laten authentiseren op afstand. SURFsecureID heeft niet de ingebouwde mogelijkheid om remote vetting toe te passen. Dit kan opgelost worden door zelf een procedure in te richten. Het fysiek langsgaan bij een servicebalie kan gezien worden als een obstakel voor sommige docenten.

4.3.2: iDIN

Het idee achter iDIN en Idensys is dat de gebruiker bij het aanvragen van deze middelen zijn identiteit al laat controleren. Het authenticatiemiddel wat verkregen wordt uit iDIN of Idensys wordt dan gebruikt om in te loggen bij de organisatie. Daardoor ontstaat een principe genaamd 'derived identity' (Hulsebosch, 2017) De applicaties hebben de gebruiker al een keer gecontroleerd en dan kan er van uit worden gegaan dat deze identiteit klopt. iDIN in dit geval is een dienst wat aangeboden wordt door Nederlandse banken. De gebruiker is al ingeschreven bij zijn eigen bank en daar is al een hoge mate van zekerheid over de identiteit.

Het nadeel aan iDIN is dat het identiteitsbewijs dat geregistreerd wordt bij de organisatie misschien niet overeenkomt met het identiteitsbewijs dat genoteerd bij de organisatie is. Waar bij SURFSecureID de laatste twee cijfers van het documentnummer worden genoteerd voor eventuele audits, wordt bij iDIN niets genoteerd. Deze gegevens zijn wel bekend bij de bank maar het is maar de vraag of deze gegevens overeenkomen met de gegevens bij de organisatie. Tevens kan er verwarring ontstaan over het controleren van de naam. iDIN geeft de initialen van de gebruiker, niet de hele naam. Sommige organisaties kunnen hier problemen mee krijgen aangezien de namen van hun werknemers voluit geschreven staan. Hierdoor kan er verwarring ontstaan over de aangeleverde initialen en de opgeslagen naam bij de organisatie. Daarnaast brengt iDIN ook een privacy probleem met zich mee. De banken die het aanbieden zijn in staat om de logins in te zien en bij te houden.

4.3.3: Idensys

Idensys was tot en met december 2018 het publiek-private Nederlandse systeem voor elektronische identificatie (eID). De overheid ontwikkelde in dat kader de Nederlandse standaard voor toegang tot digitale dienstverlening en uitwisseling van persoonlijke informatie met de overheid en het bedrijfsleven. De Nederlandse overheid werkte samen met het bedrijfsleven om deze standaard te ontwikkelen. De gebruiker kan op drie verschillende manieren inloggen: via een sms-code, met een app of door een selfie te maken en deze op de app te plaatsen.

Idensys heeft een groot nadeel: de pilot waarin Idensys getest werd is per december 2018 gestopt. Er wordt binnen de overheid nu besproken wat de verdere plannen zijn over dit systeem.

4.3.4: DigiD

DigiD is een inlogmethodiek die gebruikt wordt door de overheid. DigiD stuurt het Burger Service Nummer (BSN) door naar de organisatie waar er ingelogd wordt. Alleen organisaties die gerechtigd zijn om het BSN te gebruiken mogen gebruik maken van DigiD. DigiD verandert binnenkort naar eIDAS Substantial (Hulsebosch, 2017).

Het grootste nadeel van DigiD is dat er per login betaald moet worden. Dit is slechts 0,12 cent per login, maar als dat door 4900 werknemers een aantal keer per dag uitgevoerd gaat worden lopen de kosten hoog op. Daarnaast is er ook het probleem dat de bestaande organisatie aangepast moet worden. Een externe broker, Logius, moet DigiD implementeren bij de bestaande ICT organisatie. Dit proces zal veel tijd in beslag nemen. Daarnaast komen daar kosten bij. Als laatste is er nog het probleem dat onderzoekers in het buitenland, die misschien geen Nederlandse identiteit hebben, geen gebruik van DigiD kunnen maken.

4.3.5: IRMA

IRMA is de naam voor het systeem wat de identiteit van de gebruiker kan bewijzen. De naam IRMA staat voor: *I Reveal My Attributes*. IRMA stelt de gebruiker in staat om online, via de mobiele telefoon, bepaalde attributen wel te laten zien, waaronder leeftijd, BSN of naam, maar ook om andere attributen juist niet te laten zien zoals emailadres of telefoonnummer. IRMA beschermt

daarmee de gebruiker zijn privacy. Deze privacybescherming zit in al sinds het begin van de ontwikkeling in het systeem, en wordt daarom ook *privacy by design* genoemd.

De app heeft een eigen PIN-code die nodig is voor het gebruik. De attributen van de gebruiker worden gedownload in de IRMA-app op de telefoon. Het attribuut verkrijgen gaat via een website, QR-code of persoonlijk aan een balie. De gebruiker kan de attributen downloaden in de IRMA app op zijn telefoon. De organisatie die attributen uitgeeft heet een *attribuut uitgever*.

Volgens de ontwikkelaar van IRMA kunnen er verschillende attribuut uitgevers zijn, zoals:

- De nationale overheid, of een gemeente, voor attributen als: naam, adres, geboortedatum, BSN, rijbevoegdheid, categorie van inkomen, etc.;
- Banken en verzekeringsmaatschappijen, voor attributen als: bank- en verzekeringsnummers, soort verzekering, etc.;
- Internet serviceproviders en telecomoperators, voor: email-adressen, telefoonnummers en IP-nummers;
- Facebook / Google / Apple / Amazon / Microsoft voor login gegevens;
- Grote of kleine webshops, voor eigen klantenkaarten met bijbehorende status, coupons, etc.
- Bedrijven en andere organisaties, voor attributen ten behoeve van verfijnde rol-gebaseerde toegangscontrole;
- Ziekenhuizen en andere gezondheidsinstellingen, voor regulering van toegang niet alleen voor het eigen personeel, maar ook voor patiënten;

De stichting Privacy by Design onderhoudt een publiek register van alle beschikbare IRMA-attributen. De Radboud Universiteit zal dan moeten aangeven welke attributen zij willen zien alvorens de gebruiker kan inloggen op de applicaties.

Het nadeel aan IRMA is dat het nog niet beschikbaar is voor grootschalig gebruik. Privacy by Design is druk bezig om de samenwerking met meer attribuut-uitgevers aan te gaan. Daarnaast is het ook nog niet duidelijk welke LoA de methodiek kan garanderen.

Het verschil tussen IRMA en iDIN/ DigiD/ Idensys:

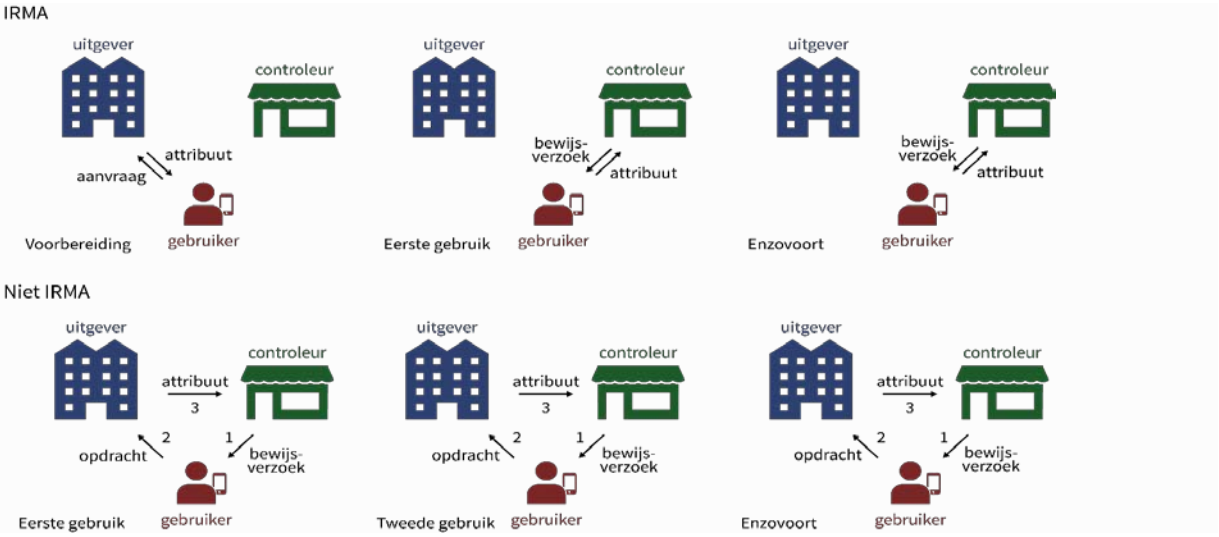
IRMA is wezenlijk verschillend van andere identity managementsystemen zoals iDIN, Idensys en DigiD. IRMA maakt namelijk gebruik van een decentrale architectuur. Wat dat inhoudt wordt door de webpagina van de Privacy by Design groep het beste uitgelegd:

"IRMA heeft een decentrale architectuur. Uw attributen zijn alleen bij u op de telefoon opgeslagen, en niet centraal op de computer van een of andere "identity broker". Wanneer u wilt bewijzen dat u ouder dan 18 bent tegenover een webshop doet u dat met IRMA rechtstreeks met die webshop, zonder tussenkomst van een "makelaar" of een "broker" of wie dan ook die hier niks mee te maken heeft. Door deze decentrale architectuur van IRMA kan niet door derde partijen bijgehouden worden:

- *welke attributen u heeft*
- *waar u die gebruikt*
- *wanneer u die gebruikt.*

Op deze manier biedt IRMA optimale privacy-bescherming, by design.

Het verschil tussen een decentrale (IRMA) en centrale (niet-IRMA) opzet wordt in figuur 4 nog eens beschreven.



Figuur 4 Werking IRMA vs andere identificatiemethoden

"Duidelijk is dat in de niet-IRMA opzet de uitgever van attributen een privacy hotspot is die bij alle transacties een vinger in de pap heeft. Bovendien kan, in de centralistische opzet, een kwaadaardige uitgever in principe uw identiteit overnemen en doen alsof hij u is. U hebt geen manier om dat tegen te houden, of zelfs maar te merken — totdat u mogelijk later met de consequenties geconfronteerd wordt. In de gedecentraliseerde IRMA-architectuur heeft u wel degelijk echte volledige controle over het gebruik van uw gegevens: u onthult zelf, rechtstreeks uw eigen attributen, iedere keer enkel na expliciete toestemming, zonder (onnodige) bemoeienis van derde partijen.

4.3.6: beoordeling vettingmethodieken met eigen criteria:

Tabel 5 bevat de uitleg van de kleuren die gebruikt zijn om de vettingmethodieken te beoordelen.
Tabel 6 bevat de resultaten van de vettingmethodieken.

Tabel 7 Scorelijst verklaring

Groen:	Voldoende.
Oranje	Twijfelachtig: Er zijn positieve punten te benoemen maar ook negatieve punten.
Rood	Onvoldoende.

Tabel 8 Beoordeling vettingmethodieken

Vettingmethodiek: →	SURFsecureID	iDIN	Idensys	DigiD	IRMA
Criteria ↓					
Gemakkelijk te gebruiken door de gebruiker.					
Gemakkelijk te gebruiken door de organisatie.					
Automatisering van het proces.					
Voldoet aan de LoA 2 en 3.					
Bruikbaar voor het grootste gedeelte van de gebruikers.					
Kosten					
Inzetbaarheid en controleerbaarheid					

4.4: Onderzoeksvraag 4

Hoe voert het Windesheim de vettingprocedure van hun medewerkers uit en hoe is hun beheer hiervan ingericht?

In dit hoofdstuk worden de resultaten uit onderzoeksvraag 4 beschreven. De resultaten geven een beschrijving van de organisatie van de gebruikte vettingmethodiek en het beheer van het Windesheim, waarom ze gekozen hebben voor deze vettingmethodiek, waarom andere vettingmethodieken zijn afgewezen en welke adviezen ze hebben voor de Radboud Universiteit.

De I, R1 en R2 in de citaten staan voor “interviewer”, “respondent 1” en “respondent 2”.

4.4.1: Organisatie vettingmethodiek en beheer van het Windesheim:

Het Windesheim gebruikt SURFsecureID en voert de vettingprocedure als volgt uit:

1. De gebruiker logt in op www.sa.surfconext.nl en verstuurt het certificaat wat in het beeld verschijnt. SURFconext ontvangt het certificaat met de voor- en achternaam van de gebruiker en zijn/haar e-mailadres.
2. De gebruiker selecteert een token, YubiKey of Tiqr, om te registreren.
3. De gebruiker ontvangt een e-mail en klikt op de activatielink.
4. De gebruiker krijgt een activatiecode in hun werkmail.
5. De gebruiker gaat dan naar een RA bij de informatiebalie, en geeft de RA de activatiecode.
6. De RA logt in op www.ra.surfconext.nl en vult de activatiecode in.
7. De RA activeert dan het token.
8. De RA vraagt de gebruiker om een identiteitsbewijs, rijbewijs of paspoort.
9. De RA controleert of de gebruiker overeenkomt met het ingeleverde identiteitsbewijs.
10. De RA vult de laatste twee tekens in van het documentnummer op het portaal.

Een verschil met het Windesheim en de Radboud Universiteit is dat het Windesheim een kleinere campus heeft. Hierdoor is het mogelijk om op één centrale locatie, namelijk de servicebalie, het vettingpunt te plaatsen. De Radboud Universiteit heeft zeven verschillende faculteiten, allemaal met hun eigen gebouw en soms is één faculteit verdeeld over meerdere gebouwen. Hierdoor wordt het moeilijk om één centrale locatie aan te wijzen, zelfs bij één faculteit. 2FA wordt momenteel gebruikt bij het studentenregistratiesysteem, verzuimregistratie en bij het volgsysteem.

Het beheer van de 2FA en vetting is simpel ingericht. Het beheer van de gegevens wordt geregeld door SURF. Het Windesheim beheert de namen van de werknemers. Alleen de Registration Authorities (RA’s) en Registration Authority Administrators Authorities (RAA’s) kunnen inloggen op de server van SURF en kunnen inzien wie er allemaal geregistreerd zijn.

4.4.2: Redenen voor aannemen SURFsecureID:

I: “dus eigenlijk de reden waarom jullie voor Surf hebben gekozen is omdat én het proces makkelijker te doorlopen is én er is inderdaad een eh, noem het maar even een Registratie Authority, die dan die identiteit bevestigt.” R1: “ja, voor de gebruiker is het heel helder, je hoeft alleen maar de website te geven en in feite kunnen ze zeg maar zelf al, stap voor stap precies uitgelegd wat ze moeten doen.”

De reden waarom Windesheim SURFsecureID heeft aangenomen is dat het proces zeer gemakkelijk te doorlopen is, het controleert de identiteit van de gebruiker fysiek en qua kosten is het gunstig. Tevens wordt er gebruik gemaakt van RA’s, dus aangewezen werknemers die de verantwoordelijkheid krijgen om de werknemers te verifiëren. SURFsecureID heeft het voordeel dat de organisatie van de vettingmethodiek en het beheer hiervan zodanig wordt ingericht dat de instelling er weinig last van heeft. SURFsecureID beheert het toegangsmiddel, naam en laatste zes cijfers van het document nummer. De instelling zelf hoeft dit niet bij te houden. Daarnaast is het uit

te voeren proces niet ingewikkeld, alle stappen worden aangegeven door SURF zodat de gebruiker ze enkel hoeft uit te voeren. Als laatste reden is dat SURFsecureID aangesloten kan worden op ADFS.

4.4.3: Redenen voor afwijzing andere vettingmethodieken:

R1: ” *Denk veel hogescholen Microsoft gericht zijn, we maakten ook al gebruik van die beheerders van die 2fa methode van Microsoft. Maar we hebben die dingen tegen elkaar gehouden, ja het was gewoon, we vonden het vetting proces van die Microsoft 2fa, naja, niet voldoen aan de eis die wij stelden. Wij wilden gewoon zeker weten dat een persoon hoort bij een bepaald token en zeker weet dat die persoon ook die persoon is. Dus toen kwamen we weer uiteindelijk uit bij Surf, Secure ID. Dat is MFA (Microsoft Multi-Factor-Authentication) en dat ehm, dat heb ik toen bekeken, dat is ehm, je kunt jezelf registreren bijvoorbeeld”*

Het Windesheim maakte eerst gebruik van het systeem van Vasco. Deze licentie is een aantal jaar geleden afgelopen en er moest iets nieuws voor in de plaats komen. De kosten van Vasco waren aan de hoge kant, waardoor het financieel niet meer echt aantrekkelijk was. Daarna werd MFA overwogen maar deze is uiteindelijk niet aangenomen. Het grote nadeel voor het Windesheim was dat bij MFA de gebruiker zichzelf kan gaan vetten. Er komt dan geen extra persoon of controle bij te pas die een gebruiker kan controleren. Windesheim had de eis gesteld dat er zo grondig als mogelijk wordt gecontroleerd en dat wordt dus niet gedaan bij MFA.

4.4.4: Adviezen voor de Radboud Universiteit:

R2: “We hebben er ook voor gezorgd dat het CvB erachter stond. Dat die het ook belangrijk vond. Dus dat van bovenaf kun je naar beneden toe dirigeren, dus al die managers die eronder zaten moesten ook eeh, als ze verzuim wilden registreren moesten ze nu ook 2f authentiseren, met het idee van het is belangrijk genoeg, je wilt gewoon inderdaad, het gaat wel om persoonlijke gegevens, belangrijke gegevens dus iedereen zag wel de noodzaak er van in.”

R1: “als je inderdaad tegen mensen zegt 'joh CvB heeft het besloten" dan is het gewoon klaar.”

Een groot voordeel wat het Windesheim heeft ten opzichte van de Radboud Universiteit, is dat het Windesheim al veel langer gebruik maakt van een twee-factor-authenticatie. Dat veel werknemers al werkten met 2FA was een groot voordeel, maar daar lieten ze het niet bij. Als eerste, en belangrijkste, werd vanuit het College van Bestuur (CvB) gecommuniceerd naar de medewerkers dat het vetten verplicht was. Als er vanuit het CvB wordt gezegd dat er iets gedaan moet worden, valt daar weinig tegenin te brengen.

Naast het decreet van de CvB hebben ze mails intern rondgestuurd en op hun intranet aankondigingen gezet waarin stond dat er overgestapt werd naar 2FA en wat de werknemers dan moesten doen. Daarnaast werden er op de Kerstmarkt standjes opgezet waar iedereen informatie kon ophalen en met hun vragen terecht konden.

R2: “Ja maar we hebben hier ook een aantal, dat heeft Anita (Security Manager Windesheim) *gedaan, zo'n training die security eeeh, van die acties zeg maar he. Beetje van die phishing dingen zeg maar, daar kwam ook gewoon uit dat 1 op de zoveel z'n wachtwoord geeft.”*

Wat ook heeft geholpen bij het informeren van de medewerkers is dat er veel gebruik gemaakt is van mediavoorbeelden over het uitlekken van persoonsgegevens door slordig username/password beheer van medewerkers en is er een security actie uitgevoerd waarbij er een phishing mailtje was uitgestuurd. Deze actie heeft aangetoond dat veel medewerkers en studenten in een phishing mailtje trappen, waardoor ook weer de noodzaak voor 2FA wordt aangetoond.

Hoofdstuk 5: Conclusies

In dit hoofdstuk worden de conclusies van de onderzoeksvragen beschreven. Aan het einde van het hoofdstuk wordt een terugkoppeling gemaakt met de informatie genoemd in het theoretisch kader.

5.1: Conclusie onderzoeksvraag 1:

Om de onderzoeksvraag te kunnen beantwoorden zijn de voorwaarden die genoemd zijn in de interviews samengevat in een enkele zin. De volledige toelichting van de security- en gebruikersvoorwaarden is terug te vinden in bijlage 15. Het antwoord op de onderzoeksvraag: *Wat zijn de organisatorische randvoorwaarden voor de vettingmethodiek, van zowel security- als gebruikerskant, van de Radboud Universiteit?* is als volgt:

De security voorwaarden:

1. De vettingprocedure voldoet aan de eisen van de ISO 27001.
2. Er is een mogelijkheid om toegekende toegangsmiddelen op afstand ongeldig te maken door de bevoegde beheerders.
3. Indien bij de vetting fysieke toegangsmiddelen verstrekt worden, zijn deze middelen beschermd op een beschermde locatie opgeslagen geweest.
4. Bij de uitreiking van toegangsmiddelen wordt identiteitscontrole uitgevoerd door middel van een wettelijk geldend identiteitsbewijs. Hierbij wordt vastgelegd wat noodzakelijk is voor de auditeerbaarheid, niet meer dan voor dit doel noodzakelijk is.
5. De geldigheid van toegangsmiddelen wordt na een nader te bepalen periode beperkt.
6. De vettingprocedure moet de opgestelde wettenkaders hanteren.
7. Accounts en authenticatiemiddelen worden verwijderd bij beëindiging contract.
8. LoA 2 voor normale applicaties. LoA 3 voor omgang met bijzondere persoonsgegeven.
9. De vettingmethodiek moet auditeerbaar zijn.

Gebruikersvoorwaarden:

1. De gebruikers willen op eenvoudige wijze toegang krijgen tot de applicaties die ze nodig hebben voor hun werkzaamheden.
2. De gebruiker wil zo min mogelijk extra handelingen uitvoeren.
3. De faculteiten willen een heldere voorlichting krijgen waarin het nut en belang van de twee-factor-authenticatie duidelijk wordt gemaakt.
4. Voldoende begeleiding en hulp bij het activeren van hun tokens.
5. De gebruiker moet een keuze hebben tussen verschillende tokens zodat ze zelf kunnen kiezen wat hun authenticatiemiddel wordt.
6. De gebruiker wil zo veel als mogelijk zelf controle hebben over zijn eigen digitale identiteit.

5.2: Conclusie onderzoeksvraag 2:

Het antwoord op de vraag: *Welke normen zijn relevant voor de vettingmethodiek van de Radboud Universiteit?* is als volgt:

De belangrijkste normen waar rekening mee gehouden moeten worden zijn de normen ISO 27001 en ISO 29115. De Radboud Universiteit hanteert momenteel al ISO 27001. Deze norm geeft aan de Radboud Universiteit de beschikbaarheid, vertrouwelijkheid en integriteit van hun informatie beheerst. Dat betekent dat de gegevens die de vettingmethodiek verzameld beschermd worden door de informatiebeveiliging van de Radboud Universiteit. De vettingmethodiek moet meegenomen worden in de periodieke uitvoering van de risicoanalyse & -beoordeling, waarmee specifieke organisatierisico's rond informatiebeveiliging worden weggenomen door passende beveiligingsmaatregelen.

De Radboud Universiteit wil graag LoA 2 voor reguliere processen zoals Brightspace en Osiris en LoA 3 voor kritieke bedrijfsprocessen zoals beheerservers gebruiken. De norm waarin deze LoA's vandaan komen is de ISO 29115. De risicotabel die benoemd is in de ISO 29115 kan gebruikt worden tijdens toekomstige risicoanalyses om de LoA's van nieuwe applicaties te bepalen. Deze norm is niet zozeer noodzakelijk voor de Radboud Universiteit om over te nemen, het is belangrijk om op de hoogte te zijn van deze norm en waar de LoA's vandaan komen.

5.3: Conclusie onderzoeksvraag 3:

Het antwoord op de onderzoeksvraag: *Welke van de vettingmethodieken uit het rapport "Remote Vetting for SCSA" scoort het hoogst bij de toetsingscriteria van de Radboud Universiteit?* is het volgende:

SURFsecureID scoort het hoogst in de toetsingscriteria. In de beoordeling is af te lezen dat SURFsecureID de meeste groene scores heeft gekregen ná IRMA.

Met SURFsecureID kan een organisatie de toegang tot online-diensten beter beveiligen, via twee-factor-authenticatie. Collega-instelling Windesheim gebruikt deze methodiek, maar op kleinere schaal en is zeer tevreden over de functionaliteit en toepasbaarheid van de methodiek. Hier moet wel bij vermeld worden SURF druk bezig is om de SURFsecureID dienst stevig uit te breiden. SURF is nu aan het onderzoeken of het mogelijk is om iDIN, Idensys, DigiD en IRMA aan te sluiten op de dienst zodat deze ook als authenticatiemiddel kunnen worden gebruikt.

De reden waarom er niet voor IRMA kan worden gekozen is dat het nog steeds in de ontwikkelingsfase zit. Duidelijk is inmiddels wel dat op termijn IRMA een zeer interessante optie is voor het vetten.

iDIN, Idensys en DigiD worden niet aanbevolen omdat deze het grote nadeel hebben dat de hele infrastructuur qua 2FA moet worden aangepast. Tevens worden de gegevens bij deze brokers opgeslagen en is het niet altijd even duidelijk wie allemaal bij deze gegevens kunnen en wat er mee wordt gedaan. De banken die iDIN aanbieden kunnen dan ook de transacties inzien die gedaan worden. Dit zorgt toch voor een privacyvraagstuk, de Radboud Universiteit moet bepalen of zij dit willen toestaan. Daarnaast hebben deze methodieken het nadeel dat er per login betaald moet worden.

5.4: Conclusie onderzoeksvraag 4:

Het antwoord op de vraag "*Hoe voert het Windesheim de vettingprocedure van hun medewerkers uit en hoe is hun beheer hiervan ingericht?* is als volgt:

Het Windesheim maakt gebruik van SURFsecureID en voert de vettingprocedure als volgt uit:

1. De gebruiker logt in op www.sa.surfconext.nl en verstuurt het certificaat wat in het beeld verschijnt. SURFconext ontvangt het certificaat met de voor- en achternaam van de gebruiker en zijn/haar e-mailadres.
2. De gebruiker selecteert een token, YubiKey of Tiqr, om te registreren.
3. De gebruiker ontvangt een e-mail en klikt op de activatielink.
4. De gebruiker krijgt een activatiecode in hun werkmail.
5. De gebruiker gaat dan naar een RA bij de informatiebalie, en geeft de RA de activatiecode.
6. De RA logt in op www.ra.surfconext.nl en vult de activatiecode in.
7. De RA activeert dan het token.
8. De RA vraagt de gebruiker om een identiteitsbewijs, rijbewijs of paspoort.
9. De RA controleert of de gebruiker overeenkomt met het ingeleverde identiteitsbewijs.

10. De RA vult de laatste twee tekens in van het documentnummer op het portaal.

Het beheer van de SURFsecureID gegevens ligt volledig bij SURF. Alleen de RA's en RAA's kunnen inloggen op de server met de persoonsgegevens en inzien wie er allemaal geregistreerd zijn. Het beheer van deze gegevens wordt geregeld via SURF. Het Windesheim beheert wel haar eigen werknemersgegevens, zoals naam, emailadres en werknemersnummer.

De belangrijkste adviezen die het Windesheim heeft gegeven zijn:

1. Zorg ervoor dat het CvB volledig achter het feit staat dat twee-factor-authenticatie noodzakelijk is en laat hen dit via een officieel bericht mededelen.
2. Informeer de werknemers op tijd en zorg voor een uitgebreide voorlichtingscampagne.
3. Implementeer Microsoft ADFS zodat applicaties voorzien met 2FA gemakkelijk verloopt.
4. Biedt een centraal punt aan waar werknemers langs kunnen om zich te laten vetten of technische problemen te laten oplossen.

5.5: Conclusie probleemstelling:

Het antwoord op de probleemstelling "*Welke vettingmethodiek past binnen de organisatorische randvoorwaarden van de Radboud Universiteit?"* is beantwoord aan de hand van de resultaten uit de onderzoeksvragen. Het resultaat is dat **SURFsecureID** het beste past binnen de organisatorische randvoorwaarden van de Radboud Universiteit.

SURFsecureID voldoet aan zowel de beveiligingseisen als de gebruikersvoorwaarden, zoals te zien is in tabel 9 en 10.

Tabel 9 Security eisen

Security eisen:	Voldoet aan?	Toelichting
Vettingprocedure voldoet aan de ISO 27001 en ISO 29115.	Ja.	De vettingmethodiek is in staat om opgenomen te worden in het ISMS systeem van de Radboud Universiteit. De LoA's in SURFsecureID zijn gebaseerd op de ISO 29115.
Er is een mogelijkheid om de toegangsmiddelen ongeldig te maken door de beheerders.	Ja.	De RA en RAA's hebben de bevoegdheid om de accounts te verwijderen.
Mogelijkheid om toegangsmiddelen op een beschermde locatie te leggen en toegang te beperken tot geautoriseerde personen.	Ja.	Er moet bepaald worden waar de Yubikeys opgeslagen gaan worden. Dit kan bij het Forum gedaan worden of bij de faculteiten zelf.
Identiteitscontrole uitgevoerd door middel van een wettelijk geldend identiteitsbewijs.	Ja.	Alleen rijbewijs en paspoort worden geaccepteerd.
Geldigheid van toegangsmiddelen te beperken?	Nee.	Het is nog niet mogelijk om een tijdslimiet te stellen op de accounts. De RU kan dit verhelpen door zelf een protocol op te stellen.
Vettingprocedure respecteert de opgestelde wettenkaders.	Ja.	Er worden niet meer persoonsgegevens verzameld dan naam, email en de laatste twee cijfers van het documentnummer. Deze gegevens worden beheerd door SURF en enkel de RA's en RAA's hebben toegang tot deze gegevens. Gebruiker kan gemakkelijk de gegevens inzien op aanvraag.
Waarborging recht van inzage in de persoonsgegevens van een gebruiker.	Ja.	Gebruiker kan gemakkelijk de gegevens inzien op zijn eigen telefoon en op aanvraag.
LoA 2 en LoA 3 mogelijk.	Ja.	Tiqr voor LoA 2. Yubikey voor LoA 3.
Vettingmethodiek auditeerbaar.	Ja.	SURF biedt de dienst aan en ook SURF audit. Geeft mogelijkheid tot auditen.

Tabel 10 Gebruikersvoorwaarden

Gebruikersvoorwaarden	Voldoet aan?	Toelichting
Gebruikers wil op eenvoudige wijze toegang tot de applicaties die ze nodig hebben.	Ja.	De gebruiker moet als hij inlogt op Osiris of een andere applicatie met 2Fa een scan maken met Tiqr of de Yubikey gebruiken. Dit is slechts één extra handeling bovenop de username+password.
De gebruiker wil zo min als mogelijk extra handelingen uitvoeren.	Ja.	De gebruiker hoeft alleen een QR-code te scannen of de Yubikey te gebruiken, naast de normale handeling username+password.
Voldoende begeleiding en hulp bij het activeren van token.	Ja.	Er zijn RA's aangewezen die de gebruiker kunnen helpen met eventuele problemen. Deze RA's moeten wel snel te vinden zijn op het intranet.
Gebruiker moet keuze hebben tussen verschillende tokens zodat ze zelf kunnen kiezen.	Ja.	De keuze tussen de Tiqr app of een Yubikey. Misschien na de zomer extra keuzes tussen iDIN, IRMA of een NFC-chip.
Gebruiker heeft controle over eigen digitale identiteit	Ja.	De digitale identiteit van de gebruiker staat op de telefoon en kan hij zelf ook verwijderen. Yubikey is alleen in bezit bij de gebruiker. De RA's en RAA's kunnen wel de gegevens inzien en wissen, voor de rest kunnen zij hier niks mee.
De faculteiten moeten een heldere voorlichting krijgen waarin het nut en belang van twee-factor-authenticatie duidelijk wordt gemaakt.	Ja	Dit moet door de Radboud Universiteit zelf worden gedaan. Zie "Vergroten draagvlak werknemers/ security awareness vergroten.

Het is alleen nog niet op alle punten toepasbaar. De mogelijkheid tot remote vetting is niet mogelijk met SURFsecureID. Het kan eventueel wel worden gedaan via een videoconference op een beveiligde verbinding, maar de RU moet bepalen of zij dit willen toelaten. Daarnaast biedt SURFsecureID niet de mogelijkheid om toegangsmiddelen automatisch na een bepaalde tijd te deactiveren. Dit kan verholpen worden door een protocol op te stellen waarin wordt aangegeven dat sommige toegangsmiddelen na een nader te bepalen tijd moeten worden gedeactiveerd, zodat er een nieuw vettingmoment kan plaatsvinden.

5.6: Terugkoppeling theoretisch kader

De afstudeeropdracht heeft tijdens het gehele onderzoeksproces rekening gehouden met artikel 25 van de AVG: Privacy by Design. Justitia (2018) stelt dat er bij voorbaat rekening gehouden moet worden met de privacy van de gebruikers en dat deze aandacht voor de privacy tijdens de gehele levensduur van een systeem blijft bestaan. Daarom is aan het begin van het onderzoek al vastgesteld wat de belangrijkste privacywetten waren voor de vettingmethodiek en dat deze wetten gewaarborgd moesten worden.

Zoals vernoemd in het theoretisch kader bestaat er een spanningsveld tussen privacy en security. Volgens Blonk (2017) hechten burgers veel waarde aan hun privacy maar eisen ze ook een toename

in veiligheid. SURFsecureID stelt de Radboud Universiteit in staat om zowel de belangen van de securityverantwoordelijken als gebruikers te behartigen.

Daarnaast stelt SURFsecureID de Radboud Universiteit in staat om compliant te zijn aan de genoemde wetsartikelen in het BSI (2018). De Radboud Universiteit vraagt niet meer persoonsgegevens dan noodzakelijk, de gegevens worden alleen gebruikt om de gebruiker te authentiseren en de gegevens worden veilig opgeslagen bij SURF. De Radboud Universiteit moet nog wel stappen ondernemen gebruikers te informeren over het doeleinde van het verzamelen van de gegevens en waar de gebruikers naartoe moeten als zij hun gegevens willen inzien of willen verwijderen.

Voor identity management is SURFsecureID voordelig want er hoeven geen extra gegevens bij de Radboud Universiteit opgeslagen te worden. Deze worden beheerd door SURF.

Hoofdstuk 6: aanbevelingen

Te gebruiken vettingmethodiek:

Uit het onderzoek is naar voren gekomen dat er het beste gebruik gemaakt kan worden van **SURFsecureID**.

Een groot voordeel van SURFsecureID is dat het volledig compatibel is met ADFS van Microsoft, wat betekent: 2FA door middel van SURFsecureID invoeren op applicaties is een kwestie van een hokje aanvinken. De Radboud Universiteit heeft in januari 2018 besloten om gebruik te gaan maken ADFS. Het technische platform staat klaar en wordt binnenkort geïmplementeerd. SURFsecureID kan hier makkelijk op worden aangesloten en de werknemers die al gevet zijn kunnen, als de applicaties met 2FA beschermd gaan worden, gelijk gebruik maken van deze applicaties.

Inrichting en organisatie vetting:

Om het de gebruikers zo makkelijk als mogelijk te maken om zich te laten vetten, moeten er meerdere RA-punten opgericht worden. Het zou verstandig zijn om alle faculteiten te voorzien van één of maximaal twee RA's. Deze RA's kunnen nieuwe werknemers vetten zodat deze gebruikers niet naar andere gebouwen moeten om zich te laten helpen. Tevens kunnen werknemers die problemen hebben met de Tiqr-app of hun Yubikey hier langs gaan om dit op te laten lossen. De afdelingen Personeel en Organisatie (P&O) bij de faculteiten zouden een geschikt punt zijn voor docenten en medewerkers van de desbetreffende faculteit om zich te laten vetten. Er moet wel nagevraagd worden of P&O hier de tijd en capaciteit voor heeft. In bijlage 16 zit een overzicht van de vettingprocedure, functies van de RA's en RAA's en een overzicht van de verschillende faculteiten.

Vergroten draagvlak werknemers/ Security Awareness vergroten:

De belangrijkste en meest noodzakelijke actie die nu ondernomen moet worden is steun verkrijgen vanuit de CvB. De faculteiten staan bekend om hun kritische houding en een helder besluit van de CvB om 2FA te gaan gebruiken kan helpen om de acceptatie te vergroten. De faculteiten kunnen nog zoveel bezwaren hebben, maar als de CvB meldt dat de werknemers gebruik moeten maken van 2FA en de bijbehorende vettingprocedure moeten doorlopen, kan er uiteindelijk weinig tegengewerkt worden. Wel is het enorm belangrijk om duidelijk aan te geven dat de gebruiker meerdere mogelijkheden qua authenticatiemiddelen hebben, namelijk de Tiqr-app of een Yubikey en dat de vettingprocedure volledig voldoet aan de AVG en verdere relevante wetgevingen. De gebruiker moet geïnformeerd worden dat de persoonsgegevens die opgenomen worden enkel de naam, e-mailadres, personeelsnummer en een nader te bepalen aantal tekens van het documentnummer zijn.

Een van de grootste struikelpunten tijdens de uitrol in november was dat de docenten van mening waren dat zij niet goed geïnformeerd waren over de redenen voor het kiezen voor 2FA en wat het is. Het is belangrijk om een gedegen communicatietraject en een daarmee gepaard gaande promotiecampagne te ontwikkelen en uit te voeren. Om de onderwerpen van de campagne te bepalen kan gebruik worden gemaakt van het FAQ. Hierin zijn alle prominente vragen geïnventariseerd en beantwoord. Rondom deze antwoorden kan de campagne opgericht worden. Deze FAQ is te vinden in bijlage 7.

Het Windesheim heeft een soortgelijke campagne al eens uitgevoerd en hier kan dus ook zeker naar gekeken worden. Zij hebben informatiestandjes opgericht en meerdere berichten geplaatst op het intranet. De Radboud Universiteit kan overwegen om dit ook via het intranet te verspreiden. De gebruikers moeten bewust gemaakt worden van de risico's die aan verkeerd gebruik of verlies van het toegangsmiddel verbonden zijn. Wat verder een goed middel is om de gebruiker te informeren is het vrijgeven van de resultaten van de phishing-actie in oktober 2018. Hierin wordt aangetoond dat er veel werknemers en studenten nog in phishingmailtjes trappen en zo hun inloggegevens weggeven, met alle gevolgen van dien.

De promotiecampagne moet pas uitgevoerd worden ná het besluit van de CvB. De grootschalige uitrol om werknemers vetten kan worden gedaan met behulp van de Campus Detachering, een uitzendbureau voor studenten. Dit scheelt in de kosten en de vorige ervaringen met de studenten van de Campus Detachering werden als zeer positief ervaren. Wel moet dit goed gepland en afgestemd met de faculteiten worden.

Bronnenlijst:

Auditconnect. (2018, januari 1). *ISO 27002*. Opgehaald van www.auditconnect.nl: https://www.auditconnect.nl/nl/it-audits/ISO-27002/

Benantar, M. (2018). *Access Control Systems: Security, Identity Management and Trust Models.*

Blonk, L. (2017). *Politieke perspectieven op privacy.* Utrecht: Universiteit voor Humanistiek.

Bron, R., Kummeling, H., & Muller, E. (2007). *Veiligheid en Privacy.* Den Haag: Boom Juridische uitgevers.

BSI. (2018). *General Data protection Regulation.* Nijmegen: Behavioural Science Institute.

Computable. (2018, G.D). *Hoe ga je om met de gebruikersidentiteit in de cloud?* Opgehaald van computable.nl: https://www.computable.nl/artikel/showcase-partnerzone/cloud-computing/4505425/4495863/hoe-ga-je-om-met-gebruikersidentiteit-in-de-cloud.html

Confluence. (2019, G.D). *Tecnische specificaties e4n procedures voor uitgifte van authenticatiemiddelen.* Opgehaald van afsprakenstelsel.etoegang.nl.

Cuijpers, C., & Schroers, J. (2018). *eIDAS as guideline for the development of a pan European eID framework in FutureID.* Nijmegen: Radboud Universiteit/ KU leuven.

de Baets, A. M. (2016). *The tension between privacy and security.* Groningen: RUG.

Design, P. B. (2019, Januari 1). *IRMA uitleg*. Opgehaald van www.privacybydesign.foundation: https://privacybydesign.foundation/irma-uitleg/#architectuur

Dingemans, K. (2017, Maart 14). *Coderen interview*. Opgehaald van www.scribbr.nl: https://www.scribbr.nl/onderzoeksmethoden/coderen-interview/

Dingemanse, K. (2016, April 6). *Observatie in je scriptie- wanneer kun je het gebruiken?* Opgehaald van www.scribbr.nl: https://www.scribbr.nl/onderzoeksmethoden/observatie-je-scriptie/

Dingemanse, K. (2017, Mei 5). *4 tips voor het opnemen van een interview*. Opgehaald van www.scribbr.nl: https://www.scribbr.nl/onderzoeksmethoden/opnemen-interview/

Disterer, G. (2013). *ISO/IEC 27000, 27001 and 27002 for Information Security management.* Hannover: Department of Business Administration and Computer Science, University of Applied Sciences and Arts Hannover.

Engelfriet, A. (2018, Februari 5). *AVG compliance mag allemaal nog onder AVG*. Opgehaald van ICTU.nl : https://www.emerce.nl/achtergrond/avg-compliance-mag-allemaal-nog-onder-avg-320

FAO. (2014). *Good Practice Definition.* -: FAO.

Government, U. S. (2018, Januari 1). *Proof an Identity at Level of Assurance 4.* Opgehaald van arch.idmanagement.gov: https://arch.idmanagement.gov/usecases/14_proofidentityloa4/

Hulsebosch, B. W. (2017). *Remote Vetting for SCSA.* Utrecht: SURFnet.

Infosecuritymagazine. (2016, Mei 19). *Europol: burgers zullen deel van hun privacy moeten opgeven voor veiligheid.* Opgehaald van www.infosecuritymagazine.nl:

https://www.infosecuritymagazine.nl/2016/05/19/europol-burgers-zullen-deel-van-hun-privacy-moeten-opgeven-voor-veiligheid/

Jurg, P., & Valkenburg, P. (2007). *Identity management: omgaan met elektronische identiteiten.* Sdu uitgevers bv: Den Haag.

Justititia. (2018, Januari 1). *Privacy by Design*. Opgehaald van Justitia.nl: https://www.justitia.nl/privacy/privacy-by-design

Kader. (2018). *ISO 27001.* Amsterdam: Kader.

Logius. (2018, Januari 1). *Zakendoen met Logius- Doorbelasting*. Opgehaald van Logius.nl: https://logius.nl/onze-organisatie/zakendoen-met-logius/doorbelasting

Maniam, S. (2016, Februari 19). *Americans feel the tensions between privacy and security concerns.* Opgehaald van Pew Research Center: http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/

McCallister, E., & Brackney, R. (2011). *ISO/ IEC DIS 29115 Information Technology- Security Techniques.* Hamburg: OASIS.

Meindersma, C. (2018, April 4). *De 6 grondslagen van de AVG*. Opgehaald van www.charlotteslaw.nl: https://www.charlotteslaw.nl/de-6-grondslagen-van-de-avg/

Microsoft. (2017, Mei 31). *When to create a federation server*. Opgehaald van docs.microsoft.com: https://docs.microsoft.com/nl-nl/windows-server/identity/ad-fs/design/when-to-create-a-federation-server

NEN. (2013, April 1). *Betekenis van een ISO-norm voor compliance management.* Opgehaald van www.nen.nl: https://www.nen.nl/web/file?uuid=7cb3670a-e21e-47e8-90c6-caee413d2b35&owner=ccdd2a27-7f28-43b1-a3cb-d01e2bf2a56a&contentid=161765

Niek Reulink, L. L. (2005). *Kwalitatief Onderzoek.* Nijmegen: Radboud Universiteit.

Privacybescherming: gedrag versus wetgeving. (2015, September 11). Opgehaald van Computable: https://www.computable.nl/artikel/opinie/zorg/5587528/1509029/privacybescherming-gedrag-versus-wetgeving.html

Schildmeijer, R., Samson, C., & Koot, H. (2005). *Burgers en hun privacy.* Amsterdam: TNS.

Strome, D. (2017, Juli 26). *Configure a federation trust exchange.* Opgehaald van docs.microsoft.com: https://docs.microsoft.com/en-us/exchange/configure-a-federation-trust-exchange-2013-help

Swaen, B. (2013, Oktober 10). *Wat is kwalitatief en kwantitatief onderzoek?* Opgehaald van www.scribbr.nl: https://www.scribbr.nl/onderzoeksmethoden/kwalitatief-vs-kwantitatief-onderzoek/

Swaen, B. (2016, november 16). *Betrouwbaarheid in je scriptie.* Opgehaald van www.scribbr.nl: https://www.scribbr.nl/onderzoeksmethoden/betrouwbaarheid-je-scriptie/

TUV. (2018). *Wat is ISO 27001?* Den Haag: TUV Nederland.

van der Harts, E. (2018, Juli 12). *RA rollen toewijzen*. Opgehaald van wiki.surfnet.nl: https://wiki.surfnet.nl/display/SsID/RA-rollen+toewijzen

van der Linde, X., & de Graaf, J. (2017, Juli 17). *Factsheet eIDAS*. Opgehaald van www.ictu.nl: https://www.ictu.nl/sites/default/files/documents/ICTU%20Factsheet%20eIDAS.pdf

van Est, R., Kool, L., & Timmer, J. (2015). *De datagedreven samenleving.* Den Haag: Rathenau Instituut.

van Leeuwen, D. (2016, December 16). *Het spanningsveld tussen veiligheid en privacy.* Opgehaald van infosecuritymagazine.nl: https://www.infosecuritymagazine.nl/2015/12/16/het-spanningsveld-tussen-veiligheid-en-privacy/

Veenstra, S. (2017, September 2). *iDIN en Idensys nieuwe identificatie diensten onder de loep*. Opgehaald van blog.mirabeau.nl: https://blog.mirabeau.nl/nl/articles/idin_en_idensys%3A_nieuwe_identificatie_diensten_onder_de_loep/d7VTNX3vawcAYYkKIiy4Y

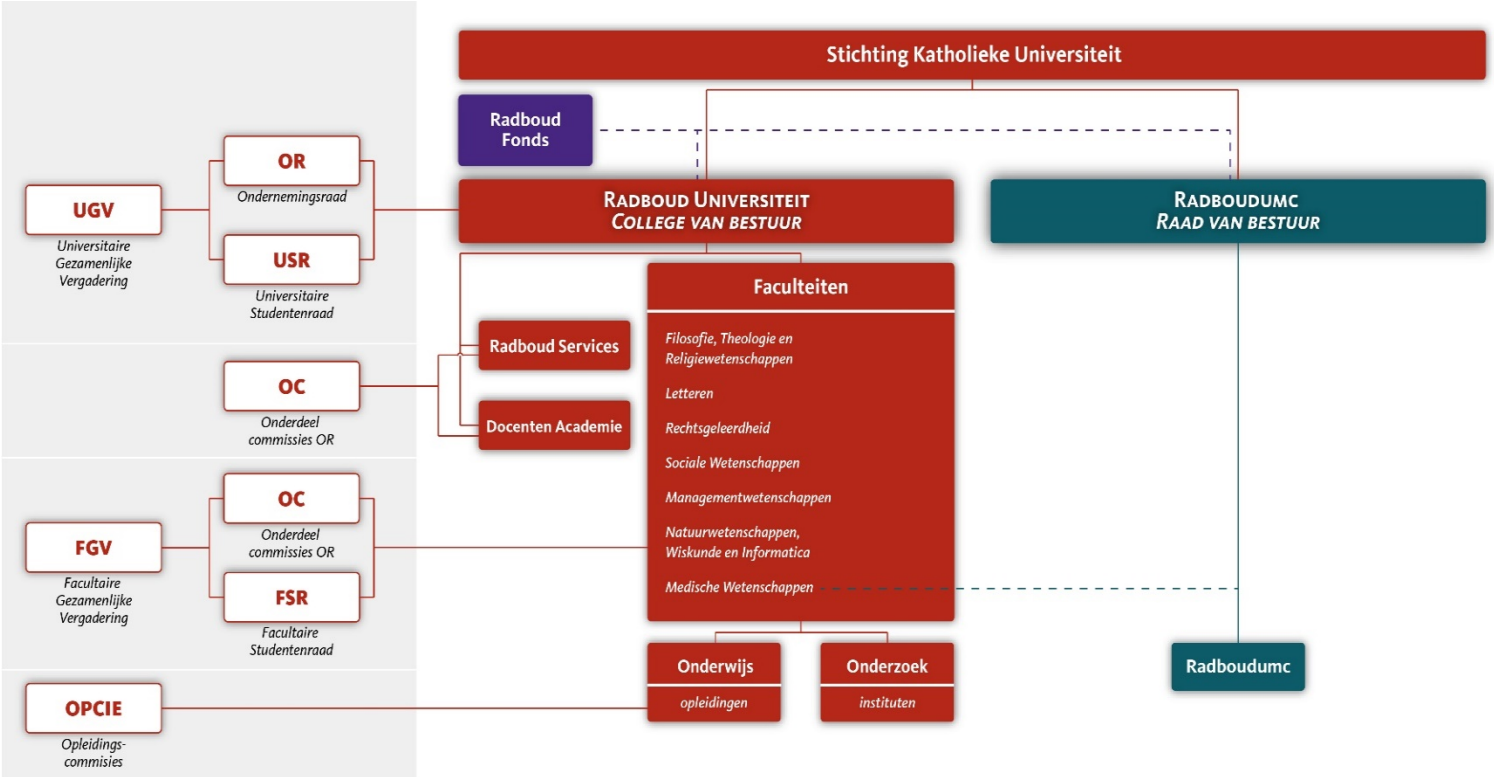
Verhoeven, N. (2011). Wat is onderzoek?

Verhoeven, N. (2014). *Wat is onderzoek?* Den Haag: Boom Lemma uitgevers.

Wokke, A. (2017, September 25). *Diensten moeten 14 cent gaan betalen als gebruiker inlogt op DigiD*. Opgehaald van www.tweakers.net: https://www.auditconnect.nl/nl/it-audits/ISO-27002/

Bijlages

Bijlage 1: Organogram



Bijlage 2: Belanghebbenden

Organisatie-onderdeel	**Waarom?**
Verantwoordelijke partij	-
Personeelszaken	Registratie en identiteitscontrole medewerkers.
Leidinggevenden	Zij gaan over de rollen en autorisaties voor medewerkers.
Identitymanagement	Uitvoerend in registratie, toekennen van accounts en wachtwoorden. Op langer termijn ook andere authenticatiemiddelen.
Uitvoerende partij:	
International Office	Controle identiteiten buitenlandse studenten, verlenen van toegang tot de opleiding.
Dienst Studentenzaken	Controle identiteit en toegang verlenen tot de opleiding voor studenten.
Service-eigenaren	Verlenen toegang aan geautoriseerde medewerkers op basis van authenticatie.
ICT	Technische implementatie, logging en monitoring van toegangspogingen.
Projectmanagement	Uitvoering van vetting.
Helpdesk en servicedesk	Gebruikerscontact, vragen beantwoorden , problemen oplossen, gastaccounts verstrekken.
Bibliotheek	Toegang tot diensten en content waar licentievoorwaarden aan vast zitten.
Portiers, sportcentrum, anderen die toegang geven tot faciliteiten	Controle personen en identiteiten.
CISO, privacyfunctionaris, Security manager	Toezicht op juiste implementatie en veiligheid en privacy in de gaten houden.
Auditing:	
Auditdienst	Controle.

Bijlage 3: Mail ICT Security Manager

Algemeen

- stappenplan

Het schema bij aanschaf, implementatie, in gebruik name van nieuwe ict-middlen of procedures is dat je naast de functionele wensen altijd kijkt naar normen en regels, die hierbij een rol spelen. Wat moet het kunnen en hoe kan dat efficiënt en veilig, en binnen een acceptabel budget.

- Classificeren en risicoanalyses

Dat betekent dat je in het voortraject al een classificatie moet doen van de gevoeligheid van systeem en data die verwerkt worden. Daaruit volgt welke wetten en normen van toepassing zijn.
Bij persoonsgegevens zal altijd de AVG van toepassing zijn (en afhankelijk van het veld: de telecommunicatiewet, auteurs- en portretrechten, cookiewet etc.). Verder zal een organisatie heel vaak gegevens willen afschermen vanwege bijvoorbeeld concurrentiegevoeligheid, dat is geen wettelijke regel, maar noodzakelijk voor het voortbestaan.
Een volgende stap is een risico-analyse (in geval van de AvG een PIA).

- Concretiseren, uitwerken
Met de wetten en normen en de risico-analyse als basis, zal er een pakket van eisen opgesteld moeten worden, waaraan zal moeten worden voldaan. Voor een aanbesteding is het een must dit goed te doen. Anders krijg je van die projecten waar verderop allerlei aanvullende eisen komen en dus het budget overschreden zal gaan worden.
Het omzetten van vaak vage normen en wetten naar concrete maatregelen en eisen is een lastige stap. Dat hangt mede af van de wat voor ict-middel precies ingevoerd moet gaan worden en de omgeving waarin dit gebeurt.
Er zijn meerdere organisatie die hiervoor richtlijnen, uitwerkingen etc. hebben opgesteld.
NCSC met richtlijnen en whitepapers, BIG/NORA van de Nederlandse gemeenten, BIHO/ SURF voor het hoger onderwijs, PIVB (platform nformatiebeveiliging) gericht op bedrijfsleven en publieke organisaties). Hieruit kun je plukken om een passende set concrete eisen en maatregelen op te stellen voor jouw organisatie of jouw project. Het kan soms lastig zijn als je een voorloper bent, maar dat volg je het idee.

- Implementatie en toetsen

Als het goed is, kun je nu beginnen de invoering. Voor de definitieve IPN (in productiename) moet je nog testen of het systeem inderdaad voldoet, functioneel en qua (beveiligings)eisen.
Dat betekent dus pentensten en audits voor de veiligheid en pilots voor functionaliteit.
(Als het niet voldoet, eis je dat het op orde komt voordat je de rekening betaalt. Dat kun je natuurlijk alleen als er niet voldaan is aan het pakket van eisen waaraan de leverancier moest voldoen. Anders zit je zelf in de problemen.)

Vetting

Bovenstaand schema/ volgorde kun je ook voor Vetting-procedures aanhouden.

De normen en wetten noemt Ronald al. Onder de securityeisen. De AvG als belangrijkste wet in dit opzicht. De AvG speelt bij vetting een dubbele rol.

1 De AvG kan om een vetting vragen: er is een adequate beveiliging van persoonsgegevens vereist, dus goede controle over de autorisaties. In een PIA stel je het LOA vast en het risico dat

toegangsmiddelen verkeerd verstrekt worden. Dus dat je een vetting moet doen om dat risico af te dekken..

2) Bij het proces van vetting worden identiteiten gecontroleerd en persoonsgegevens verwerkt.
dus de procedure en de dataverwerking zelf moet ook AvG compliant zijn.
(moet je de uitvoerders van de vetting eerst ook vetten?????)

Ronald noemt nog enkele securityvoorwaarden:

De securityvoorwaarden uit die in het interview naar voren komen zijn:

- *Zekerheid dat de persoon die het token krijgt, ook daadwerkelijk die persoon is.*
- *De vettingprocedure past binnen de normen van de ISO 27001.*
- *Verbeterde intrekking middelen van werknemers. werklaptops en werktelefoons beter geregistreerd.*
- *Waarborging recht van inzage in de persoonsgegevens van een persoon.*

De volgende stap is dus zoals boven beschreven: algemene eisen en normen concretiseren in maatregelen voorschriften voor de daadwerkelijke uitvoering. En daarbij ook toepasbaar maken voor de organisatie en de omgeving waarbinnen die vetting uitgevoerd moet worden.
In het interview worden al enkel van di organisatie specifieke en omgevingsfactoren genoemd.
- de dubbelrollen die studenten soms hebben (assistent, mentor)
- de menselijke factor: het draagvlak
- op afstand vetten mogelijk maken

Er zijn eisen en maatregelen, die vrij algemeen gelden en er zijn specifieke voor de RU. Ik begin er maar eens wat op te schrijven

1. Indien bij de vetting fysieke toegangsmiddelen verstrekt worden, zijn deze middelen beschermd opgeslagen geweest. Toegang tot deze opslag is beperkt tot geautoriseerde personen en wordt gemonitord en is traceerbaar.
2. Indien bij vetting digitale toegangsmiddelen verstrekt worden, geldt overeenkomstig: toegang tot het systeem waarin dit opgeslagen is, is beperkt tot geautoriseerde personen, wordt gemonitord en is traceerbaar.
3. Bij de uitreiking van toegangsmiddelen wordt identiteitscontrole uitgevoerd door overlegging van een wettelijk geldend identiteitsbewijs. Hierbij wordt vastgelegd wat noodzakelijk is voor de auditeerbaarheid, niet meer dan voor dit doel noodzakelijk is..
4. Er is een procedure voor innamen van toegekende toegangsmiddelen en de registratie hiervan.
5. Er is een mogelijkheid toegekende toegangsmiddelen op afstand ongeldig te maken.

De geldigheid van toegangsmiddelen is in tijd beperkt.

Bijlage 4: Interviewvragen CISO

1. Wat wil de Universiteit bereiken met de identiteitscontrole?
2. Welke normen moeten in acht worden genomen bij het vetten?
3. Zijn er ook specifieke beveiligingsnormen van toepassing bij het vetten?
4. Maakt de Universiteit gebruik van Levels of Assurance?
5. Zo ja, welke is vereist?
6. Zo nee, wat voor classificatie hebben de gegevens gekregen?
7. (Doorgaand op antwoord nee) hoe is deze classificatie opgesteld?
8. Wie moeten verantwoordelijk zijn voor het beheer van het proces?
9. Welke wetten dienen in acht genomen te worden?
10. Is het Radboud bekend met eIDAS?
11. Zo ja, welke maatregelen zijn genomen om compliant te zijn?
12. Wil de Universiteit gebruik maken van E-herkenning?
13. Is er een privacy impact analyse uitgevoerd over de 2fa, zo ja, wat zijn hier de resultaten van?
14. Zijn er autorisatie-matrices, waarin de rollen en bevoegdheden van medewerkers vastgelegd zijn?
15. Hoe is de intrekking van middelen (telefoons, Yubikeys, Ipads) geregeld?
16. Is er een update-beleid voor de systemen, software en protocollen en wordt dat gecontroleerd en ge-audit?
17. Bij authenticatieprocessen wordt veel versleuteling (TLS etc) gebruikt en certificaten uitgewisseld.
    Zijn er eisen vastgesteld voor die transportprotocollen en voor de lengte/sterkte van de certificaten?

Bijlage 5: Interviewvragen Project Manager

1. Wat zijn de meest gehoorde/besproken bezwaren over het volgen van een technisch identiteitscontrole-proces?
2. Hoe belangrijk vinden de gebruikers de handhaving van de nieuwe AVG?
3. Waar zien de gebruikers het meest tegenop bij het registreren van hun identiteit?
4. Hebben docent voorkeur voor bepaalde apps?
5. Hoe is het gesteld met de Security Awareness van de docenten?
6. Zijn docenten zich bewust van de redenen wáárom er gevet moet worden?
7. Hoe verloopt de voorlichting van de docenten?
8. Ziet de gebruiker het nut van het security middel? Waarom wel of waarom niet?
9. Accepteert de gebruiker dat hij/zij extra handelingen moet verrichten? (gebruik token en de controle op de identiteit)
10. Wat verwacht de gebruiker aan ondersteuning bij vragen of problemen?
11. Is de gebruiker bereid om een privé device te gebruiken?
12. Is de organisatie (ook een rol als gebruiker) bereid middelen als token te verstrekken? En zo ja, op welke schaal? Medewerkers, studenten?
13. Is de organisatie bereid om servicedesk(s) in te richten voor het vetting proces, ook voor grote aantallen gebruikers? (dit is een lastige om de juiste personen voor te interviewen)

Bijlage 6: Axiaal codering CISO en Project Manager

CISO:

	A	B
1	*Codering*	*Inhoud*
2	Security eisen	Alles wat gebruikt kan worden om de gewenste security eisen op te stellen.
3	Noodzakelijke wetten	Alle wetten die belangrijk zijn om compliant aan te zijn.
4	Struikelpunt: Onduidelijkheden	
5	Normen:	Alle normen die genoemd worden in de tekst die van belang of gewenst zijn.
6	LOA	Het gewenste LOA niveau.
7	Struikelpunt: Technische problemen	Alles wat te maken heeft met de technische problemen die de Universiteit momenteel ondervindt.
8	Struikelpunt: Menselijke factor	Alle opmerkingen die gaan over problemen veroorzaakt door een menselijke factorbinnen de universiteit
9	Voorwaarden Vetting	Alles wat de wensen/ voorwaarden voor het vettingsysteem duidelijk maakt.
10	Overig	Alle informatie die niet direct van belang is voor het beantwoorden van de onderzoeksvraag, maar wel belangrijk en/of interessant is voor het gehele onderzoek.
11	Suggesties voor vetting	Hiermee worden ideeën voor vettingmethoden in de tekst met gelabeld.

Project Manager 2FA:

	A	B	C
1	Hoofdthema	Subthema	Toelichting
2	Wensen	Radboud	Met dit hoofdthema worden alle wensen die in de tekst besproken zijn gemarkeerd. Daarin wordt nog het onderscheid gemaakt of de wens vanuit de Radboud Universiteit zelf komt of vanuit de gebruikers.
3		Gebruiker	
4	Probleemstukken Organisatie	Lastige organisatiestructuur	Met dit hoofdthema worden alle probleemstukken in de organisatiestructuur in de tekst gemarkeerd. Hieronder
5		Cultuur	
6	Noodzakelijkheden		Dit hoofdthema geeft aan welke acties ondernomen moeten worden/ geadviseerd worden als het vettingproces opgesteld/ geïmplementeerd gaat worden.
7	Andere vettingmethodiek	Redenen voor afwijzing	Dit hoofdthema geeft de vettingmethodieken aan in het interview. Tevens wordt in axiaal laag 2 de reden(en) voor afwijzing of aannemen gemarkeerd.
8		Redenen voor aannemen	
9	Problemen gebruikers	Tijd	Dit hoofdthema omvat alle problemen van de gebruikers, genoemd in de tekst. Hierin worden de subthema's tijd, moeite en onbegrip in onderverdeeld. Dit geeft meer duidelijkheid in de type problemen die de gebruikers ondervinden.
10		Moeite	
11		Onbegrip	
12	Overig		Alle informatie wat interessant is maar niet direct onder de andere hoofdthema's vallen.

Bijlage 7: Frequently Asked Questions

Vraag	*Antwoord*
Wat doet deze app precies?	Deze app scant de QR-code die wordt weergegeven op het beeldscherm als de docent moet inloggen.
App is geactiveerd, wat nu?	Als de docent inlogt op Osiris moet deze eerst een username+ password invoeren. Daarna komt er een QR-code op het beeldscherm, deze dient gescand te worden met de app. Daarna vult u uw pin in en kan de docent door.
Waarom noteren jullie de laatste zes cijfers/letters van mijn rijbewijs/paspoort?	Deze cijfers worden gelinkt aan uw account voor audit-doeleinden. Deze registratie geeft extra verificatie over de identiteit van de gebruiker.
Moet ik dit ook echt doen?	Ja. Osiris gaat gebruikmaken van 2FA, als u geen token gaat gebruiken kunt u geen cijfers invoeren.
Kan dit ook zonder telefoon?	Ja. Met Yubi-key of Ipad/ Samsung tablet.
Wat moet ik doen als ik een nieuwe telefoon krijg?	Dit proces nogmaals doorlopen. Kan op aangegeven punten.
Hoe installeer ik de app?	Android/Windows Phone: Ga naar de playstore Apple: Appstore. Volg de aanwijzingen op het scherm en volg daarna de aanwijzingen in de mail/ ga naar een helpdesk.
Ik wil geen Apple/Samsung/Google-account, wat nu?	Gebruikmaken van de Yubi-Key of een account aanmaken.
Wat is mijn wachtwoord?	Dat weten wij niet.
Kan ik hier nu ook mee digitaal ondertekenen?	Ja.
Kan ik mijn digitale identiteit inzien?	Ja. Deze staat op de telefoon. Deze kan zelf verwijderd worden.
Kan ik mijn gegevens inzien en beheren?	Ja, deze staan op uw telefoon of heeft u in bezit.

Bijlage 8: Originele beoordelingslijst SURF:

3.3. Assessment criteria

Remote vetting solutions have to fulfil to a number of criteria. These criteria are derived from interviews and discussion sessions with SURFnet and stakeholder institutions.
Criteria for remote vetting are:

1. Easy to use by the user: if the user experiences inconveniences during remote vetting he may cancel the process. For instance, many users would like to be able to obtain a SCSA token outside office hours. Compared to the current practice, the ease of use of the solutions from a user perspective can be either better, equal or worse.
2. Easy to organize by the institution: it must be easy for the institution to enrol, deploy, initiate, or arrange a remote vetting solution. Compared to the current practice, the ease of use of the solutions from an institution perspective can be either better, equal or worse.
3. Limited impact on current SCSA service: how easily can the remote vetting solution be integrated with the current SCSA service, what needs to be adapted technically or organisationally by SURFnet, is it a one-off (e.g. software improvement) or continuous (e.g. audit process) effort? Solutions have no, limited or large impact on the current SCSA service provisioning.
4. Straight-through processing: the possibility to vet for the user's identity in a fully automated manner without human interference. More automation means shorter vetting lead times and improves the user experience. It also provides more efficiency, scalability and less errors (e.g. due to manual processing of personal information). For bulk enrolment scenario's this is very relevant. The automation capabilities of the vetting process are less, similar or better than the current situation offers.
5. Sufficient penetration rate: as many potential target users as possible must be able to go through a remote vetting process. Certain user groups may not be able to execute the remote vetting process because they lack certain functionality that is required for remote vetting (e.g. they use a phone that does not support NFC or do not have a Dutch bank card). The penetration rate is higher, equal or lower compared to what the existing SCSA solution for vetting.
6. Sufficient level of authentication assurance: the outcome of the remote vetting must provide sufficient assurance in the identity of the user (which on its turn will provide a higher authentication assurance). Solutions must achieve a level of assurance that at least correspond to LoA 2 and LoA 3 as used by SCSA.
7. Costs: the cost of the solution is reasonable. The current service desk costs are estimated to be about a minimum of 5 Euro per vetting[10]. User costs are also involved. However, these are more difficult to quantify as the costs for students are different than for employees. Therefore, the user's costs are taken into in the ease of use criterion above. There are other costs as well, such as development costs (only once), licensing costs (recurring), and technology/hardware costs. However, these costs are expected to be similar for all solutions. The focus therefore will be on the costs for vetting the user. Consequently, the costs assessment of remote vetting solutions will be rated as higher, similar or lower than 5 Euro. Specific, significant additional costs will be mentioned during the assessment if needed.
8. Controllability/auditability: the ability to control the remote vetting process in such a way that it is implemented by all institutions in an unambiguous manner including the ability to audit the process for accountability purposes. The controllability/auditability of remote vetting solutions is better, similar or worse than what SCSA currently offers.
9. Future proof: Is the solution future proof and does it have a sufficient maturity level?

Bijlage 9: Toetsingscriteria van de Radboud Universiteit:

Criteria	*Toelichting*	*Hoe is dit beoordeeld?*
Gemakkelijk te gebruiker door de gebruiker:	Als een medewerker het proces om een token te verkrijgen te moeilijk vindt, is deze sneller geneigd om te stoppen met het proces.	Zelf de vettingprocedure doorlopen.
Gemakkelijk te gebruiken door de organisatie:	Het moet gemakkelijk zijn voor de RU om de vettingmethodiek uit te zetten , te gebruiken, op te nemen in de lopende processen en de mogelijkheid bieden om aan remote vetting te doen.	Met informatie op de webpagina van de ontwikkelaar onderzocht en besproken met de Project manager 2FA.
Automatisering van het proces:	De mogelijkheid om de identiteit van een medewerker te vetten door middel van een geautomatiseerd proces, waar zo min als mogelijk menselijke hulp bij nodig is. Een geautomatiseerd systeem kan grotere hoeveelheden aanvragen sneller verwerken en heeft minder kans op falen door menselijke fouten zoals het verkeerd aflezen van identiteitsbewijzen of foutief invoeren van gegevens.	Met informatie verstrekt vanuit de ontwikkelaar.
LoA 2 en LoA 3 mogelijk:	De onderzochte vettingmethodiek moet voldoen aan LoA 2 en/of LoA 3.	De informatie van de ontwikkelaar en/of uit het SURF-rapport waren gebruikt om aan te geven of deze methodieken LoA 2 en 3 konden faciliteren.
Bruikbaar voor het grootste gedeelte van de gebruikers:	Zoveel als mogelijk werknemers moeten in staat zijn om de vettingprocedure te kunnen ondergaan. Sommige werknemers zijn misschien niet in bezit van smartphones of hebben geen Nederlandse bank.	Voor SURFsecureID en IRMA: Informatie over de gebruikers van de Project Manager 2FA. Voor iDIN en Idensys: Informatie van de ontwikkelaars en aanbieders.
Kosten:	Hoeveel kost de vettingmethodiek per gevette medewerker en wat kost het om het systeem te implementeren?	Informatie van de ontwikkelaars en aanbieders van de vettingmethodieken.
Inzetbaarheid en controleerbaarheid:	De mogelijkheid van een vettingprocedure om snel organisatie-breed ingezet en beheerd te worden en gemakkelijk bekeken en beoordeeld te worden tijdens een audit.	Informatie van de ontwikkelaars en aanbieders van de vettingmethodieken.

Bijlage 10: Interview Windesheim vragen

1. Aanleiding voor het gebruikmaken van 2fa
2. Waar wordt de 2fa voor gebruikt?
3. Wat is de gebruikte vettingmethodiek?
4. Hoe zijn jullie op deze methodiek gekomen?
5. Welke methodieken zijn nog meer getest?
6. Vetten jullie ook op afstand?
7. Hoe verloopt dat proces?
8. Hoe verzeker je dat de identiteit van buitenlandse studenten kloppen?

Bijlage 11: axiaal codering Windesheim

fx

	A	B	C
1	Hoofdthema	Subthema	Uitleg
2	Awareness	Werkwijze	Deze codering geeft aan welke methoden/manieren Windesheim heeft gebruikt om de awareness van haar medewerkers bij te spijkeren. Deze methoden kunnen worden gebruikt om de awareness van de medewerkers van de Radboud Universiteit te bevorderen.
3	Vetting methodiek	Redenen voor aannemen	Dit hoofdthema wordt gebruikt om de verschillende vettingmethodieken mee aan te geven. Het subthema geeft de redenen voor aannemen of afwijzing aan. Daarnaast is er een subthema voor waarin het gebruik van de vetting wordt gemarkeerd.
4		Redenen voor afwijzing	
5		Gebruik	
6	Interessante opmerkingen	Namen	Dit is een overige categorie. Hierin worden zaken aangemerkt die eventueel interessant zijn voor het onderzoek.
7		Systemen	
8	Inrichting beheer		Deze codering geeft aan dat het stuk uitleg bevat over de inrichting van het beheer.
9	Security issue		Deze codering geeft security problemen van het Windesheim aan.

Bijlage 12: Uitwerking LoA's ISO 29115

LoA 1:

Als er gekozen wordt voor LoA 1, is ervoor gekozen om weinig vertrouwen te stellen in de identiteit van de gebruiker. Deze LoA wordt gebruikt wanneer er een minimaal risico is bepaald voor de specifieke applicatie. De impact van een fout van de authenticatie of misbruik van een identiteit zal vrij laag zijn. De identificatiemethode die hoort bij deze LoA is een username + password. De gebruiker mag een eigen username en password verzinnen en beheren.

LoA 2:

Bij LoA 2 is er bepaald dat er een zekere mate van vertrouwen in de identiteit van de gebruiker moet zijn. Deze LoA wordt gebruikt als er een gemiddeld risico wordt ervaren als de identiteit misbruikt wordt. Succesvolle authenticatie wordt gerealiseerd doordat de gebruiker een beveiligd authenticatieproces moet doorgaan en daarmee bewijst dat de gebruiker de juist identiteit heeft. De organisatie moet wel al maatregelen hebben genomen om de kans op eavesdroppers[6] en man-in-the-middle-attacks te mitigeren. Tevens moeten er maatregelen genomen zijn om de opgeslagen identiteitsgegevens te waarborgen tegen diefstal. Een voorbeeld van LoA 2 is username+password en SMS-controle. (SURF, 2018)

LoA 3

LoA 3 houdt in dat er een hoog vertrouwen moet zijn in de identiteit van de gebruiker. Deze LoA wordt gebruikt als er een significant risico is bij misbruik van de identiteit. Deze LoA zal multi-factor authenticatie gebruiken. De mate van waarheidsgetrouwe identiteiten hangt af van de gekozen verificatie manier. Alle informatie verkregen uit de verificatie van identiteiten moeten cryptografisch versleuteld worden. Een voorbeeld van LoA 3 is de Yubikey (SURF, 2018).

LoA 4:

LoA 4 is de hoogste LoA beschikbaar. Hierbij moet de identiteit van de gebruiker zeer betrouwbaar zijn. Er is namelijk een groot risico bij het misbruiken van de identiteit. LoA 4 lijkt in grote lijnen veel op LoA 3, maar het grote verschil is dat bij LoA 4 er gebruik gemaakt moet worden van biometrische gegevens, zoals een vingerafdruk of een irisscan en moet de apparatuur waarop de gegevens staan volledig fraude- en diefstalbestendig zijn.

[6] Een ICT risico waarbij een individu digitale communicatie onderschept die niet voor hem bedoeld is. (https://www.techopedia.com/definition/13612/eavesdropping)

Bijlage 13: Vettingprocedures van de vettingmethodieken

SURFsecureID:

1. De gebruiker logt in op www.sa.surfconext.nl en verstuurt de attributen met de persoonsgegevens wat in het beeld verschijnt. SURFsecureID (SURF zelf) ontvangt het certificaat met de voor- en achternaam van de gebruiker, werknemersnummer en zijn/haar e-mailadres.
2. De gebruiker selecteert een token, YubiKey of Tiqr, om te registreren.
3. De gebruiker ontvangt een e-mail en klikt op de activatielink.
4. De gebruiker krijgt een nieuwe activatiecode in hun werkmail.
5. De gebruiker gaat dan naar een RA, in dit geval de servicebalie, en geeft de RA de activatiecode.
6. De RA logt in op www.ra.surfconext.nl en vult de activatiecode in.
7. De RA activeert dan het token.
8. De RA vraagt de gebruiker om een geldig identiteitsbewijs, rijbewijs of paspoort.
9. De RA controleert of de gebruiker overeenkomt met het ingeleverde identiteitsbewijs.
10. De RA vult de laatste twee cijfers in van het documentnummer op het portaal.
11. De RA activeert dan het token, het documentnummer is nu gelinkt met de naam en emailadres van de gebruiker.

iDIN:

1. Gebruiker gaat naar de applicatie waar hij moet inloggen;
2. Gebruiker kiest iDIN als authenticatiemiddel en selecteert zijn bank;
3. Gebruiker logt in op de iDIN app en scant de QR-code op het scherm;
4. App geeft een scherm met de vraag of de gebruiker wil inloggen op deze pagina;
5. Gebruiker drukt op accepteren en vult zijn persoonlijke pin in;

Idensys:

1. De gebruiker vult zijn persoonlijke informatie in op het registratie portaal van de Idensys authenticatie service provider (denk aan gemeentes of bedrijven als Isala, Pazio, BKR, CZ en Zilveren Kruis.) De gebruiker dient wel al een account bij de betreffende service provider te hebben.
2. De gebruiker maakt een 1 cent iDeal betaling.
3. Idensys authenticatie service provider vergelijkt de persoonlijke informatie verkregen uit de iDeal betaling met de informatie van het gebruikersaccount.
4. De gebruiker installeert de mobiele app en registreert deze app door middel van een QR-code dat wordt gegenereerd door het registratie portaal.
5. De app ontvangt persoonlijke informatie en vraagt aan de gebruiker om deze gegevens te controleren.
6. De app vraagt de gebruiker om een foto van het identiteitsbewijs of een scan van de NFC-chip in het paspoort.
7. De app vraagt om een selfie.
8. De app start een video sessie en geeft willekeurige aanwijzingen aan de gebruiker. (zoals: draai het hoofd naar links, rechts, knik, lach, spreek de volgende woorden uit) Deze video zorgt ervoor dat de provider kan controleren of er daadwerkelijk een persoon achter de aanvraag zit.
9. De app zendt de informatie naar de service provider.
10. Idensys provider vergelijkt de foto op het identiteitsbewijs met de selfie.
11. Idensys provider controleert of de gebruiker de aanwijzingen heeft opgevolgd in de video.

12. Idensys provider activeert de gebruiker zijn authenticatie token.

DigiD:

1. De gebruiker meldt zich aan voor DigiD +SMS op www.digid.nl.
2. De gebruiker vult zijn persoonlijke informatie in (waaronder BSN, naam, geboortedatum, telefoon nummer), genereert een wachtwoord en ontvangt een activatiebericht op de gebruiker z'n telefoon.
3. De gebruiker activeert dit bericht. Nu is de mobiele telefoon gekoppeld aan de gebruiker z'n DigiD account.
4. Een activatiecode wordt gegenereerd en wordt per brief doorgestuurd naar het adres van de gebruiker, wat verkregen is uit de Basisregistratie Persoonsgegevens.
5. De gebruiker activeert DigiD+sms met deze code.
6. De gebruiker gaat weer naar www.digid.nl en installeert de DigiD app.
7. De gebruiker scant de QR-code op DigiD met de app.
8. De app genereert een code die op de website moet worden ingevoerd door de gebruiker.
9. De gebruiker moet een PIN-code verzinnen. De app is nu verbonden met de gebruiker zijn DigiD app.

Als het Assurance niveau verhoogd moet worden kan dit ook via DigiD.

1. De gebruiker dient weer in te loggen op mijn.digid.nl met de app.
2. De gebruiker scant de QR-code en logt in met de pin.
3. De gebruiker wordt gevraagd de chip in zijn paspoort te scannen met de NFC scanner van de telefoon.
4. Het verkregen NFC met persoonlijke informatie wordt vergelijken met de informatie in de Basisregistratie Persoonsgegevens.
5. Als de verificatie succesvol is, wordt het assurance niveau verhoogd.
6. De gebruiker kan dan weer inloggen met de app en pincode.

IRMA:

1. Gebruiker downloadt IRMA app van www.privacybydesign.foundation.
2. Gebruiker verzint zijn eigen pincode van de app.
3. Gebruiker gaat naar de attribuut uitgever en geeft aan dat hij attributen wil overnemen.
4. Attribuut uitgever geneert een QR-code en de gebruiker scant deze.
5. Gebruiker gaat akkoord met de attributen die worden gegeven.
6. Attributen worden op de telefoon geladen en kunnen gebruikt worden door de gebruiker om zich te authentiseren bij de betreffende organisatie.

Bijlage 14: Beoordelingen vettingmethodieken

SURFsecureID:

Criteria	Beschrijving	Beoordeling
Gemakkelijk te gebruiken door de gebruiker	Het proces is makkelijk te volgen aan de hand van de opgegeven informatie PDF. De gebruiker moet wel naar een RA-punt om zijn token te activeren, wat als grote moeite kan worden beschouwd. Door deze punten op veel plaatsen te zetten kan deze weerstand worden verminderd.	
Gemakkelijk te gebruiken door de organisatie.	SURFsecureID sluit aan op SURFconext, wat al organisatie-breed wordt gebruikt. Als er ook nog gebruik gemaakt gaat worden van ADFS zal het aansluiten van 2FA op applicaties makkelijker verlopen.	
Automatisering van het proces.	De werknemers moeten één voor één worden gevet, dit zal meer tijd in beslag nemen dan een geautomatiseerd proces. Op afstand vetten is moeilijk. Tevens is het invoeren van de gegevens meer vatbaar voor fouten aangezien het door mensen wordt ingevuld.	
Voldoet aan de gewenste LoA's	Zowel LoA 2 (Tiqr) en LoA 3 (Yubikey) kunnen hier gemakkelijk worden geregeld.	
Bruikbaar door het grootste gedeelte van de gebruikers	Iedereen die geen smartphone heeft voor Tiqr kan gebruik maken van een Yubikey. Enige nadelen aan de vettingmethodiek zijn dat het aantal Yubikeys bij de RU beperkt zijn en dat remote vetting moeilijk te regelen is. SURF is momenteel bezig met het testen van meerdere inlogmanieren om op afstand te kunnen vetten, waaronder iDIN, Idensys, IRMA.	
Kosten	460 euro exclusief btw per maand bij 1000 tot 5000 werknemers.[7]	
Inzetbaarheid en controleerbaarheid	Omdat de RU al gebruik maakt van SURFconext is dit makkelijk organisatie-breed in te zetten. De laatste zes cijfers van de documentnummers kunnen worden gebruikt bij een audit om te achterhalen welk persoonsbewijs aan het account verbonden is. Daarnaast is SURFsecureID volledig ISO 27001 compliant.	

[7] https://www.surf.nl/diensten-en-producten/surfsecureid/index.html

iDIN:

Criteria	Beschrijving	Beoordeling
Gemakkelijk te gebruiken door de gebruiker	Erg gemakkelijk. De gebruiker heeft al een inlogmiddel wat sterke authenticatie heeft. (Bankpas) Daarnaast biedt iDIN de mogelijkheid tot remote vetting, maar dan moet de gebruiker wel een Nederlandse bank hebben.	
Gemakkelijk te gebruiken door de organisatie.	Relatief makkelijk te gebruiken. Er zijn geen lokale en fysieke RA's nodig om een token te activeren en het beheer van de persoonsgegevens wordt door de banken gedaan. Het grote nadeel is wel dat de gehele inloginfrastructuur opnieuw ingeregeld moet worden. Er dient een iDIN-overeenkomst te worden afgesloten met een acquirer (ondernemersbank) of een Digital Identity Service Provider (DISP). Daarbij moet het proces ingebed worden in de bestaande bedrijfsprocessen en dat heeft allemaal bijkomende kosten. Daarnaast heeft deze externe partij inzicht in de persoonsgegevens van de gebruiker en kan inzien welke transacties hij allemaal maakt. Dat levert weer een privacy probleem op.	
Automatisering van het proces	Omdat men al een bank account heeft hoeft er niet een extra aanmelding plaats te vinden. Dit leidt tot een korter vetting proces. Daarnaast gebeurt het vetten op afstand.	
Voldoet aan de gewenste LoA's	Met iDIN kan LoA 2 worden gegarandeerd. LoA 3 is mogelijk om te behalen volgens iDIN, maar de Radboud Universiteit moet aangeven of zij iDIN betrouwbaarder dan een Yubikey vinden. Daarnaast verloopt de remote vetting via de browser en dat is weer vatbaar voor een MitB[8].	
Bruikbaar voor het grootste gedeelte van de gebruikers	Ongeveer 86% van de Nederlandse bevolking heeft een bank account. Er is een hele grote kans dat veel werknemers dan gebruik van iDIN kunnen maken. Het nadeel is wel dat buitenlandse werknemers die geen Nederlandse bankrekening hebben hier geen gebruik van kunnen maken.	
Kosten	Per transactie kost het 30 cent. Hoe meer attributen een organisatie vereist, hoe duurder het zal worden. Daarnaast komen nog kosten voor het implementeren van het systeem.	
Inzetbaarheid en controleerbaarheid	iDIN wordt gecontroleerd en beheerd door de onafhankelijke partij (de bank). De gebruiker kan zelf bij zijn gegevens. Als er een audit wordt gepleegd kan de authenticatie aanvraag vanuit iDIN en overeenkomst met het organisatie account worden aangetoond. Maar dat neemt niet weg dat het ingeleverde persoonsbewijs bij de bank misschien niet overeenkomt met de gegevens bij de Radboud Universiteit.	

[8] Man-in-The-Browser (MiTB) Een ICT dreiging waarbij een Trojaans paard een webbrowser infecteert om vervolgens tijdens het internetbankieren of inloggen op sites de webpagina's verandert of zelfstandig transacties uit te voeren. (Bar-Yosef, Noa. 2010)

Idensys:

Criteria	Beschrijving	Beoordeling
Gemakkelijk te gebruiken door de gebruiker	De gebruiker kan inloggen met zijn Idensys account. Alleen moeten gebruikers zichzelf gaan aanmelden bij Idensys providers. Afhankelijk van de gekozen vetting methode kan het vrij snel gaan. De hoeveelheid handelingen kan wel een obstakel zijn.	
Gemakkelijk te gebruiken door de organisatie.	Het vetten hoeft niet meer fysiek plaats te vinden, Idensys heeft dat al gedaan. Alleen dient de organisatie wel de infrastructuur aan te passen.	
Automatisering van het proces	De afwezigheid van fysiek vetten en de mogelijkheid voor remote vetting zorgt ervoor dat gebruikers zich sneller kunnen laten controleren als ze een token aanvragen.	
Voldoet aan de gewenste LoA's	Met Idensys kan LoA 2 worden behaald. LoA 3 wordt (nog) niet aangeboden. Daarnaast verloopt de remote vetting via de browser en dat is weer vatbaar voor een MitB[9].	
Bruikbaar door het grootste gedeelte van de gebruikers	Iedereen kan zich registreren bij een Idensys provider. Afhankelijk van de gekozen identificatiemethode zal het registratieproces snel zijn.	
Kosten	Er zijn kosten om een makelaar in te huren. Hoeveel er per transactie moet worden betaald is onbekend.	
Inzetbaarheid en controleerbaarheid	De organisatie die Idensys aanbiedt is verantwoordelijk voor het beheer van de persoonsgegevens. De ontwikkeling en het beheer van Idensys vinden plaats binnen de besturing van een publiek-private samenwerking. Aangezien Idensys onderdeel is van eHerkenning en aangeboden wordt door Rijksoverheid zal deze een audit kunnen doorstaan.	

[9] Man-in-The-Browser (MiTB) Een ICT dreiging waarbij een Trojaans paard een webbrowser infecteert om vervolgens tijdens het internetbankieren of inloggen op sites de webpagina's verandert of zelfstandig transacties uit te voeren. (Bar-Yosef, Noa. 2010)

DigiD:

Criteria	Beschrijving	Beoordeling
Gemakkelijk te gebruiken door de gebruiker	De gebruiker kan inloggen met zijn DigiD account. Veel mensen hebben dit al.	
Gemakkelijk te gebruiken door de organisatie.	Het beheer van de gegevens wordt door Logius gedaan. De RU zou dan zelf niet de gegevens hoeven beheren. DigiD moet wel worden aangesloten met behulp van een externe broker, dus moet de interne organisatie aangepast worden. Het stappenplan is te vinden op https://logius.nl/diensten/digid/aansluiten-op-digid.	
Automatisering van het proces	Er zijn geen mensen nodig om de gebruikers te vetten, dat moet de gebruiker zelf doen tijdens een geautomatiseerd proces. Dit zorgt ervoor dat veel mensen tegelijkertijd zich kunnen identificeren.	
Voldoet aan de gewenste LoA's	LoA 2 wordt met de normale inlogmethode vervuld. Als er wordt gekozen voor DigiD Substantial, wordt LoA 3 vervuld.	
Bruikbaar door het grootste gedeelte van de gebruikers	Veel gebruikers zullen al een DigiD account hebben. Alleen buitenlandse werknemers, die geen Nederlandse identiteit hebben kunnen hier geen gebruik van maken.	
Kosten	0,117[10] euro per succesvolle inlogpoging, exclusief BTW. Er zijn 4921 werknemers die meerdere keren op een dag zullen inloggen op een applicatie. Dat wordt veel te duur.	
Inzetbaarheid en controleerbaarheid	Logius is verantwoordelijk voor het beheer van de persoonsgegevens. De gebruiker kan snel bij zijn gegevens. Aangezien Idensys onderdeel is van eHerkenning en aangeboden wordt door de overheid zal deze een audit kunnen doorstaan. Daarnaast vereist Logius ook nog een interne controle van de organisatie als DigiD aangesloten moet worden.	

[10] https://logius.nl/onze-organisatie/zakendoen-met-logius/doorbelasting

IRMA:

Criteria	Beschrijving	Beoordeling
Gemakkelijk te gebruiken door de gebruiker	Door de aanwijzingen te volgen op het scherm is het inladen van de attributen een gemakkelijk proces. Enige wat vereist is, is een goede 4G/3G/ Wi-Fi verbinding.	
Gemakkelijk te gebruiken door de organisatie.	IRMA wordt aangesloten op SURFconext, wat al gebruikt wordt door de Radboud Universiteit.	
Automatisering van het proces	Omdat het via een applicatie gaat, is er geen menselijke factor nodig qua controleren. Het kan ten allen tijden, overal en wanneer een gebruiker het wil.	
Voldoet aan de gewenste LoA's	Onbekend. Heeft nog verder onderzoek nodig.	
Bruikbaar door het grootste gedeelte van de gebruikers	Er kunnen veel verschillende attributen worden opgevraagd bij verschillende vertrouwde instanties als de gemeente, banken, werkgever.	
Kosten	Geen. IRMA is een open source software, volledig gratis in gebruik[11].	
Inzetbaarheid en controleerbaarheid	De gebruiker heeft volledige controle over zijn gegevens. De gebruiker kan tevens bepaalde limieten aangeven over informatie die verkregen is uit de betrouwbare bronnen. De attribuut uitgevers kunnen allemaal een audit doorstaan. De Radboud Universiteit moet aangeven welke attributen zij willen inzien alvorens de gebruikers toegang krijgen tot de applicaties. Als zij attributen willen inzien die de Radboud Universiteit zelf heeft, zal deze methodiek een audit bij de Universiteit zelf doorstaan.	

[11] https://privacybydesign.foundation/irma-uitleg/#onderwerp. "*Het IRMA systeem is open (source) en gratis beschikbaar en is in principe door iedereen te gebruiken.* "

Bijlage 15: Volledige toelichting organisatorische randvoorwaarden.

Securityvoorwaarden:

1. *Het vettingproces voldoet aan de opgestelde eisen van de ISO 27001:*

De norm NEN-ISO/IEC 27001 beschrijft hoe informatiebeveiliging procesmatig kan worden ingericht. Verder stelt de norm specifieke eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd ISMS. Onderdeel hiervan is het periodiek uitvoeren van een risicoanalyse & -beoordeling, waarmee specifieke organisatierisico's rond informatiebeveiliging worden geborgd en weggenomen door passende beveiligingsmaatregelen.

2. *Er is een mogelijkheid om toegekende toegangsmiddelen op afstand ongeldig te maken door de bevoegde beheerders.*

De vettingmethodiek moet de mogelijkheid bieden om de tokens/authenticatiemiddelen op afstand te deactiveren als dat nodig is.

3. *Indien bij de vetting fysieke toegangsmiddelen verstrekt worden, zijn deze middelen beschermd op een locatie opgeslagen geweest. Toegang tot deze opslag is beperkt tot geautoriseerde personen en wordt gemonitord en is traceerbaar.*

De toegangsmiddelen dienen op een plaats opgeslagen te worden waar alleen bevoegde personen toegang tot hebben. De toegang moet ook door middel van logging bijgehouden worden, zodat het duidelijk is wie toegang heeft en de toegangsmiddelen heeft uitgedeeld.

4. *Bij de uitreiking van toegangsmiddelen wordt identiteitscontrole uitgevoerd door middel van een wettelijk geldend identiteitsbewijs. Hierbij wordt vastgelegd wat noodzakelijk is voor de auditeerbaarheid, niet meer dan voor dit doel noodzakelijk is.*

Bij het uitreiken van de toegangsmiddelen moeten de gebruikers zich identificeren door middel van een geldig paspoort, rijbewijs of, voor de buitenlandse docenten, een verblijfbewijs. De gegevens die worden vastgelegd zijn enkel geschikt voor de audit. Er morgen niet meer gegevens worden vastgelegd dan nodig is, in dit geval enkel de naam, documentnummer en e-mailadres.

5. *De geldigheid van toegangsmiddelen wordt na een nader te bepalen periode beperkt.*

De vettingmethodiek moet in staat zijn om de toegangsmiddelen na een nader te bepalen tijd te deactiveren, zeker als het om middelen gaan die toegang tot kritische applicaties geven.

6. *Het vettingproces moet de opgestelde wettenkaders respecteren/ hanteren.*

Vanaf 25 mei 2018 is er in de hele Europese Unie een nieuwe privacywetgeving van kracht. De AVG geeft inwoners van de EU meer invloed op wat er met hun privacygevoelige informatie gebeurt en wat bedrijven, overheden en organisaties ermee doen. De Radboud Universiteit moet kunnen aantonen dat zij handelt in overeenstemming met de AVG, de Universiteit heeft namelijk een verantwoordingsplicht (ISC, 2018). De AVG heeft een aantal voorwaarden die hieronder kort worden samengevat.

- Artikel 5, 6 en 7 AVG: Gebruik persoonsgegevens alleen waarvoor ze zijn verzameld.

Voordat de RU persoonsgegevens gaat verzamelen, moet duidelijk zijn omschreven voor welk doeleind die gegevens worden verzameld. de RU mag niet voor ieder doel persoonsgegevens verzamelen. De verwerking van persoonsgegevens moet een juridische grondslag hebben.

- Artikel 5 en 25 AVG: Sla niet meer persoonsgegevens op dan nodig.

De persoonsgegevens mogen alleen verzameld en gebruikt worden voor een bepaald doel. Bewaar dus geen extra informatie omdat dat misschien handig is. De persoon in kwestie heeft het recht zijn of haar gegevens in te zien.

- Artikel 6 AVG: Sla persoonsgegevens niet langer op dan nodig.

Bepaal wettelijk bewaartermijn voor de opgeslagen gegevens. De gegevens mogen niet langer bewaard worden dan noodzakelijk.

- Artikel 5, 24, 32 AVG: Sla persoonsgegevens veilig op.

De RU moet ervoor zorgen dat er geen onbevoegden bij persoonsgegevens kunnen komen. Versleutel USB-sticks, vermijd gratis clouddiensten als Dropbox en hanteer een clean-desk-policy. (ISC, 2018)

- Artikelen 7, 8 en 9 AVG: Juistheid van de gegevens en informeren betrokkenen

Verwerkte gegevens moeten juist zijn en geactualiseerd zijn waar en wanneer nodig. Er moet ook direct gereageerd worden op verzoeken van gerechtigden om inzage, correctie en verwijdering van de gegevens.

- Artikel 15 AVG :

Mensen hebben recht op inzage in hun persoonsgegevens. Zij hebben het recht om naar de verwerkte gegevens op te vragen en in te zien.

- Artikel 28 Verwerkersovereenkomst:

Een verwerkersovereenkomst regelt de verantwoordelijkheden bij de verwerking van persoonsgegevens als een bedrijf voor de verwerking een derde partij inschakelt. Wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene gewaarborgd.

Naast de AVG zijn er nog een aantal wetten waaraan compliant de Radboud Universiteit Compliant moet zijn. Deze wetten zijn als volgt:

- Cookiewet:

Als er gebruik gemaakt wordt van website, zal er ook gebruik worden gemaakt van cookies. Door de cookiewet zal de webpagina verplicht moeten vermelden dat er gebruik wordt gemaakt van cookies.

- Portretrecht

Als er gebruik wordt gemaakt van foto's voor bijvoorbeeld werknemers pasjes, zal men te maken krijgen met de portret- en auteursrechten. Dit houdt in dat diegene van wie de foto is volledige controle heeft over zijn/haar foto's en wat daar mee gebeurt.

7. *Accounts worden verwijderd van middelen bij beëindiging contract.*

De accounts die geregistreerd staan op de bedrijfsmiddelen als laptops, telefoons en tablets die gebruikt worden door medewerkers moeten bij de beëindiging van het contract worden verwijderd. Dit dient gedaan te worden bij het inleveren van de bedrijfsmiddelen. Tevens moeten de accounts van de medewerker gedeactiveerd worden door de beheerders van de accounts.

8. *LoA 2 voor normale applicaties. LoA 3 voor omgang met bijzondere persoonsgegeven.*

Voor reguliere gebruikersdiensten als mail, eduvpn en Brightspace wordt LoA 2 gehanteerd, oftewel username+password en 'something you have' als de Tiqr app of een sms-code. LoA 3 wordt gehanteerd voor toegang tot beheerservers, onderzoeksdatabases en Registration Authorities.

9. *De vettingmethodiek moet auditeerbaar zijn.*

De vettingmethodiek moet gebruik maken van logging. Er moet inzicht zijn in de personen die toegang hebben tot de gegevens en wat er met de gegevens gebeurd en wie de gegevens bewerkt. Het proces moet zodanig transparant en gedocumenteerd zijn dat het een audit makkelijk doorstaat.

Gebruikersvoorwaarden:
1. De gebruikers willen op eenvoudige wijze toegang krijgen tot de applicaties die ze nodig hebben voor hun werkzaamheden.

De gebruikers hebben aangegeven dat zij graag makkelijk toegang kunnen krijgen tot de applicaties die zij nodig hebben om hun werkzaamheden uit te voeren. Dat betekent dat er dus niet veel opdringerige maatregelen getroffen moeten worden wat het inloggen onnodig lang en moeizaam maakt.

2. *De gebruiker wil zo min mogelijk extra handelingen uitvoeren.*

Met extra handelingen wordt niet alleen het inloggen bedoeld, maar ook de handelingen die nodig zijn om geauthentiseerd te worden. Een lange vettingprocedure zal niet enthousiast ontvangen worden door de medewerkers die gevet moeten worden.

3. *De faculteiten een heldere voorlichting geven waarin het nut en belang van de twee-factor-authenticatie duidelijk wordt gemaakt.*

Een van de grootste struikelpunten waar nu tegenaan wordt gelopen is dat het niet duidelijk is wát twee-factor-authenticatie is en wáárom dit geïmplementeerd wordt. Een voorlichting over twee-factor-authenticatie en de daarbij behorende vettingprocedure bij de werknemers van de faculteiten zal helpen deze wens te vervullen.

4. *Voldoende begeleiding en hulp bij het activeren van hun tokens.*

Enkel voorlichting geven aan de medewerkers is niet voldoende. Het aanbieden van voldoende begeleiding door RA's bij het vetten zal ervoor zorgen dat de docenten het proces als prettig zullen ervaren. Tevens wil men dat er een punt is waar zij gemakkelijk informatie kunnen opvragen over het vettingproces en wat er gedaan moet worden.

5. *De gebruiker moet een keuze hebben tussen verschillende tokens zodat ze zelf kunnen kiezen wat hun token wordt.*

Als er twee-factor-authenticatie geïmplementeerd wordt, zal het waarschijnlijk helpen om de medewerker de keuze te geven tussen verschillende tokens, in dit geval de Tiqr-app of een Yubikey. Er zijn namelijk een aantal docenten die uit verschillende overtuigingen, ideeën of voorkeuren liever niet hun persoonlijke telefoon willen gebruiken voor de Tiqr-app. Deze docenten moeten dan de kans krijgen om een vervangend middel te gebruiken, zoals de Yubikey.

6. *De gebruiker wil zo veel als mogelijk zelf controle hebben over zijn eigen digitale identiteit.*

Een veelgehoorde klacht is dat de gebruikers niet weten waar hun gegevens opgeslagen worden en wat er mee gaat gebeuren. Het is verstandig om voor een vettingmethodiek te kiezen die de gebruiker de mogelijkheid geeft om zijn of haar digitale identiteit te beheren. Dit houdt in dat zij zien wat er opgeslagen wordt over hun identiteit en dat zij dit zelf kunnen verwijderen.

Bijlage 16: Organisatie en beheer Vettingmethodiek/ procedure

Overzicht Vetting en Organisatie:

Verloop vettingprocedure:

1. De gebruiker logt in op www.sa.surfsecureid.nl met een username/wachtwoord. Het scherm geeft een certificaat aan en de optie om dit te sturen naar SURFconext. De gebruiker klikt op 'versturen' en verstuurt het certificaat. SURFsecureID (SURF zelf) ontvangt het certificaat met de voor- en achternaam van de gebruiker en zijn/haar e-mailadres.
2. De gebruiker selecteert een token, YubiKey of Tiqr, om te registreren.
3. De gebruiker ontvangt een e-mail en klikt op de activatielink.
4. De gebruiker krijgt een nieuwe activatiecode in hun werkmail.
5. De gebruiker gaat dan naar een Registration Authority, in dit geval de informatiebalie, en geeft de RA de activatiecode.
6. De RA logt in op www.ra.surfsecureid.nl en vult de activatiecode in.
7. De RA activeert dan het token.
8. De RA vraagt de gebruiker om een geldig identiteitsbewijs, rijbewijs of paspoort.
9. De RA controleert of de gebruiker overeenkomt met het getoonde identiteitsbewijs.
10. De RA vult de laatste zes cijfers in van het documentnummer op het portaal.
11. De RA activeert dan het token, de gecontroleerde identiteit van de gebruiker is nu gekoppeld aan het token.

Functies binnen de vettingmethodiek:

Functie:	**Werkzaamheden**
Registration Authority Administrator (RAA)	- Aanwijzen Registration Authorities; - Vetten werknemers; - Toezien op beheer gegevens - Intrekken accounts gebruikers
Registration Authority (RA)	- Vetten van werknemers; - Deactiveren toegangsmiddelen; - Intrekken accounts gebruikers;

Beheer:

Organisatie:	*Werkzaamheden:*
SURF	- Beheer persoonsgegevens - Beheer accounts gebruikers
Radboud Universiteit	- Beschikt over credentials die noodzakelijk zijn voor de identiteitscontrole

Overzicht vetting bij Faculteiten

Twee RA's per faculteit.

Functionaris:	*Locatie*
N.T.b	Faculteit der Filosofie, Theologie, Religiewetenschappen.
N.T.B	Faculteit der Letteren
N.T.B	Faculteit der Managementwetenschappen
N.T.B	Faculteit der Natuurwetenschappen, Wiskunde en Informatica
N.T.B	Faculteit der Rechtsgeleerdheid
N.T.B	Faculteit der Sociale Wetenschappen

Centrale vettinglocaties/ ICT ondersteuning (optioneel)

Locatie	*Toelichting*
ISC Forum gebouw	Faculteit der Natuurwetenschappen, Wiskunde en Informatica zou hier langs kunnen om zich te laten vetten of met problemen als C&CZ dit niet kan faciliteren.
C&CZ	Faculteit der Natuurwetenschappen, Wiskunde en Informatica heeft zijn eigen IT-helpdesk, er moet besproken worden of zij tijd hebben om het vetten op zich te nemen.
Universiteitsbibliotheek ICT helpdesk	Werknemers kunnen hier langs om zich te laten helpen met technische problemen of zich te laten vetten.
Studentenbalie	Voor als studenten gevet moeten worden.