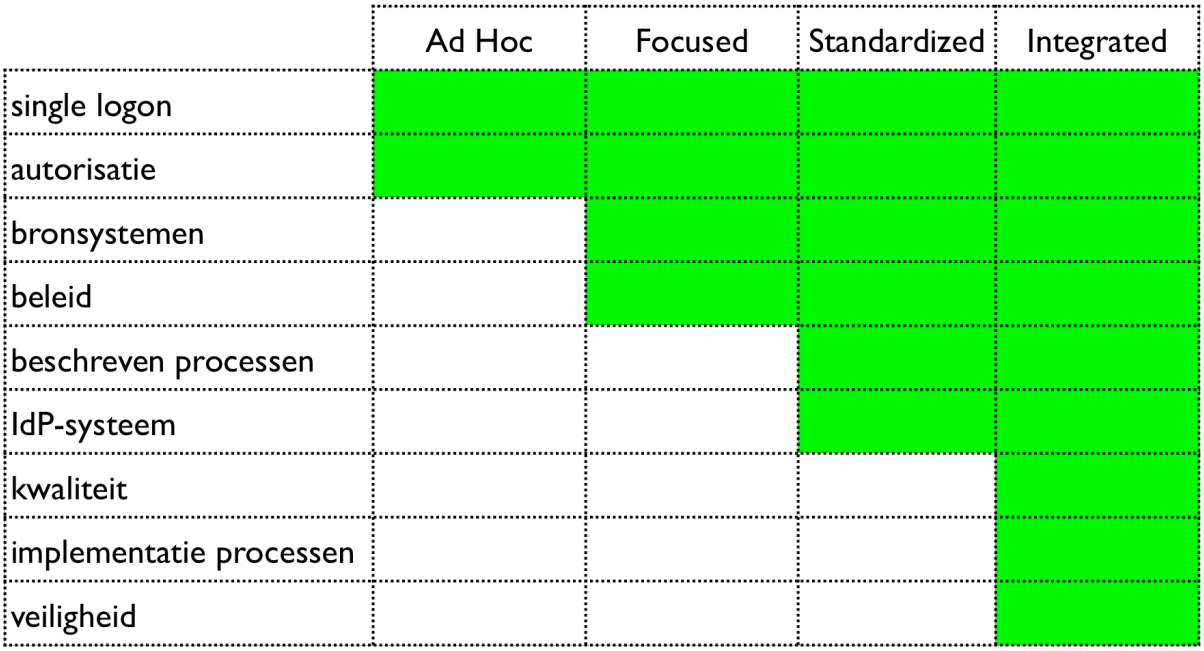
Uitleg bij de Maturity scan

Het model op hoofdlijnen

Het maturity-model gaat uit van vier categorieën die in het onderstaande plaatje horizontaal zijn weergegeven. De categorieën worden bepaald door de scores die een instelling haalt op de aspecten die verticaal zijn weergegeven. De scores worden bepaald met behulp van de vragenlijst die hieronder met 'maturity scan' wordt aangeduid.



De betekenis van de maturity niveaus is als volgt (bij ieder niveau zijn alleen de extra eisen/kenmerken beschreven die komen bovenop die van de voorgaande niveaus):

- Ad Hoc
  Een instelling heeft geen focus op identity management, maar wellicht wel een aantal praktische zaken geregeld, zoals één instellingsaccount voor meerdere diensten (misschien zelfs single sign-on), en autorisatie per applicatie.

- Focused
  Een instelling heeft een duidelijke 'focus' op identity management. Dat wil zeggen dat helder is welke systemen leidend zijn voor het bestaan van identiteiten en voor aanvullende informatie bij identiteiten, dat de provisioning naar doelsystemen is gerealiseerd en er een beleid is voor identity management waarin bijvoorbeeld de volgende zaken zijn benoemd:

    - regels voor life cycle management,
    - regels voor toegang afhankelijk van lokatie en/of type werkplek,
    - een rollenmodel
    - uitspraken over verantwoordelijkheden, beheer en onderhoud van regels en rollenmodel,

- rapportages en auditing
- welke applicaties worden aangesloten,
- hoe met federatief identity management wordt omgegaan.

- Standardized
  Een instelling heeft als onderdeel van de ingerichte provisioning een systeem beschikbaar dat als Identity Provider (IdP) kan dienen bij het aansluiten op een federatie (de SURFfederatie).
  Het beleid is vertaald naar goed beschreven processen en procedures, die zo goed mogelijk zijn geïmplementeerd.

- Integrated
  De processen en procedures zijn niet alleen geïmplementeerd, maar er is ook controle op de implementatie en ze kunnen worden herzien waar nodig.
  De kwaliteit van de data uit de bronsystemen of via andere invoer is gewaarborgd door checks en procedures.
  De beveiliging van de identity managementsystemen krijgt de benodigde aandacht en er is aan de wettelijke eisen voldaan.

Uitleg bij de aspecten

Single logon	Voor belangrijke applicaties bestaat er een generiek autenticatiemiddel
Autorisatie	Toegang tot applicaties is selectief
Geïdentificeerde bronsystemen	Voor alle identiteiten is een bronsysteem aan te wijzen;
Beleid	Er is een beleid op het gebied van identity management waarin doelen zijn beschreven, verantwoordelijkheden zijn aangegeven en is aangegeven welke systemen onderdeel uitmaken van identity management
Processen en procedures	Processen en procedures zijn beschreven en zo goed mogelijk geimplementeerd
Geschikt systeem IdP	Er is een systeem met geconsolideerde identiteiten beschikbaar, welke een integratiemogelijkheid heeft voor federatief identity management? Is het systeem voldoende beschikbaar?
Kwaliteit van de identiteiten	Zijn alle identiteiten aanwezig, is voor alle identiteiten alle relevante informatie ingevuld. Is dit verifieerbaar? En wordt het geverifieerd? Is alle informatie actueel?
Implementatie van processen en procedures	Zijn processen en procedures geïmplementeerd? Worden processen en procedures geactualiseerd?
Veiligheid	Vertrouwelijkheid en integriteit van identity management systemen en IdP-systeem.

Bepaling van de score

De maturity wordt bepaald door het geven van een score per vraag. Deze loopt van 0 tot en met 3. De vragen hebben een gewicht, waardoor een gewogen score per vraag wordt bepaald. Deze gewogen scores worden per aspect opgeteld en genormeerd naar een score vanaf 0 tot en met 10. Indien een score per aspect hoger of gelijk is aan 6 is de instelling op dat punt ‘mature’. Het eerste aspect (gerekend van boven naar beneden) waarop een instelling onder de 6 punten scoort bepaalt de ‘overall maturity’, die dan wordt bepaald doordat alleen de bovenliggende aspecten meetellen voor de ‘overall maturity’. Dus als een

instelling overal 6 of meer scoort behalve voor beleid is de maturity ‘ad hoc’. Als dan dit aspect wordt verbetert is de maturity in één keer gewijzigd naar ‘integrated’.

In de tabel hieronder zijn alle vragen weergegeven met de wegingsfactor per vraag en de manier waarop punten worden toegekend.

Maturity scan

A Simple sign on				
#	**Vraag**	**Antwoord**		**Bepaling scores**
1	Is er een unieke instellings-identiteit gedefinieerd?		1	score is 0 of 3
2	Voor welke systemen wordt dit account gebruikt? a. e-mail b. gebruikersnetwerk c. ELO d. intranet e. tentamensystemen e.d. f. draadloos netwerk g. overig		1	0 systemen = 0 punten 1-3 systemen = 1 punt 4 systemen = 2 punten 5 of meer systemen = 3 punten Hoe meer systemen er gebruik van maken, des te groter de acceptatiegraad binnen de instelling en des te groter de kans dat een medewerker of student haar/zijn instellingsID regelmatig gebruikt; dat laatste is een pre voor federatief identity management
3	Welke vormen van authenticatie gebruikt u voor dit account? a. gebruikersnaam/wachtwoord b. one time passwords c. tokens d. certificaten		1	alleen zwakke authenticatie = 2 punten ook sterke authenticatie = 3 punten zwak= userid/wachtwoord Met sterke authenticatie naast zwakke kunnen ook systemen met gevoelige informatie worden gebruikt. Dit is ook een pré voor federatief identity management
4	Zijn er nog andere identiteiten dan die instellingsidentiteit binnen de organisatie?		1	Nee = 3 punten Ja = 1 punt
5	Zo ja, kan een van deze accounts duidelijk als hoofdaccount worden aangewezen?		1	Als er een hoofdaccount is dan 3 punten, als het antwoord op 4 nee is, dan automatisch 3 punten
6	Kunt u meerdere / andere vormen van authenticatie aanbieden afhankelijk van een rol?		1	ja = 3 punten nee = 0 punten

B Autorisatie				
1	Voor welke applicaties gebruikt u autorisatie? a. e-mail b. gebruikersnetwerk c. ELO d. intranet e. tentamensystemen e.d. f. draadloos netwerk g. overig		1	0 systemen = 1 punt 1-3 systemen = 2 punten 4 of meer systemen = 3 punten Het antwoord is slechts een indicatie voor het voldoen aan autorisatievragen van diensten aanbieders op de SURF-federatie (het gaat dus om ervaring met het aanbrengen van autorisatie)
2	Is de autorisatie ad hoc bepaald of gekoppeld aan rollen en/of groepen?		2	ad hoc = 1 punt gekoppeld aan rollen en groepen = 3 punten
3	Is de autorisatie centraal of decentraal (vanuit applicatiebeheer) geregeld?		2	centraal = 3 punten decentraal = 1 punt
4	Wat voor typen identiteiten heeft u? a. medewerkers b. studenten c. externen d. alumni e. anders		2	3 typen = 1 punt 4 typen = 2 punten meer = 3 punten
5	Kunt u voor applicaties en federatief identity management) onderscheid maken tussen deze identiteiten?		2	ja = 3 punten nee = 0 punten
C Bronsystemen				
1	Wat voor bronsystemen gebruikt u? a personeelssystemen b studenteninformatiesystemen c handmatige invoer d overig		1	personeelssysteem + sis = 2 punten meer = 3 punten anders 0 punten
2	Wie mogen bij handmatige invoer gegevens muteren?		1	verantwoordelijkheden belegd = 3 punten niet belegd = 0 punten
3	Is er per identiteit een leidend bronsysteem aan te wijzen?		1	ja = 3; nee =0
4	Bent u in staat identiteiten te verrijken? (bijvoorbeeld op verzoek van een SP)		1	verrijking mogelijk = 2 punten ook verantwoordelijkheden belegd = 3 punten anders 0 punten

D Beleid 				
1	Wat ziet u als het doel van federatief identity management?		0	altijd 0 punten (telt niet mee)
2	Heeft u een identity managementbeleid voor: a. Autorisatie b. Authenticatie c. Provisionering d. Standaardisatie e. Federatief identity management f. Privacy		1	4 of meer = 3 punten 3 = 2 punten 1-2 = 1 punt anders 0 punten
3	Worden in dit beleid ook verantwoordelijkheden belegd? a. Autorisatie b. Authenticatie c. Provisionering d. Standaardisatie e. Federatief identity management f. Privacy		1	4 of meer = 3 punten 3 = 2 punten 1-2 = 1 punt anders 0 punten
4	Besteedt u (delen van) identity management uit?		0	altijd 0 punten (telt niet mee)
5	Gaat u uit van een identity management-architectuur?		1	ja = 3 punten nee = 0 punten
6	Heeft u een beveiligingsbeleid?		1	ja = 3 punten nee = 0 punten
7	Bevat uw beveiligingsbeleid een adequaat wachtwoordbeleid?		1	ja = 3 punten nee = 0 punten
8	Is er een lifecycle beleid rondom accounts?		1	ja = 3 punten nee = 0 punten
9	Hoe vaak worden uw identity management en beveiligings-beleid ge-update?		1	is een termijn bepaald = 3 punten anders 0 punten
10	Hoe actueel is uw beleid?		1	indien in de pas met antwoord op vorige vraag = 3 punten anders 0 punten
11	Wordt het beleid nageleefd?		1	goed = 3 punten middelmatig =2 slecht = 0 punten
12	Is er commitment rondom het beleid?		1	ja = 3 punten nee = 0 punten
13	Bent u bereid beleid aan te passen indien nodig om aan te sluiten bij Federatief Identity Management?		1	ja = 3 punten nee = 0 punten
14	Is er een beleid rondom het evalueren en actualiseren van uw processen en procedures?		1	ja = 3 punten nee = 0 punten

	IGI GROUP	SURF NET

E Processen en procedures				
1	Zijn er processen gedefinieerd voor het registreren van: a. nieuwe medewerkers b. nieuwe studenten c. externen die een account nodig hebben d. alumni e. nieuwe systemen		1	4 of meer = 3 punten 3 = 2 punten 1-2 = 1 punt anders 0 punten
2	Zijn er vaste regels voor gebruikersnamen, e-mailadressen etc.?		1	ja = 3 punten nee = 0 punten
3	Zijn er processen voor verrijking? a. door ondersteunend personeel b. selfservice		1	2 = 3 punten 1 = 1 punt geen = 0 punten
4	Zijn er processen voor lifecycle management geïmplementeerd?		1	voor alle identiteiten = 3 punten deels = 1 punt geen = 0 punten
5	Zijn er processen voor beschikbaar stellen van identiteiten aan derden?		1	ja = 3 punten nee = 0 punten
6	Zijn er processen voor genereren van nieuwe wachtwoorden: a. via support b. via selfservice met het oude wachtwoord c. via een set van vragen d. sms/e-mail		1	ja = 3 punten (ook vergeten wachtwoorden) nee = 0 punten
7	Hoe vaak ververst u gegevens vanuit bronsystemen?		1	real time = 3 punten (enkele minuten of minder) < 2 uur = 2 punten dagelijks = 1 punt anders 0 punten

8	Hoe vaak ververst u gegevens d.m.v. verrijking of selfservice?		1	real time = 3 punten (enkele minuten of minder) < 2 uur = 1 punt anders 0 punten
9	Hoe actueel zijn uw processen en procedures?		1	laatste jaar = 3 punten 1-2 jaar = 2 punten anders 0 punten
10	Hoe vaak worden ze gereviewed?		1	jaarlijks = 3 punten ad hoc = 1 punt niet = 0 punten
11	Zijn er rapportages beschikbaar over: a. aantal identiteiten b. aantal wijzigingen op identiteiten c. aantal externen		1	ja = 3 punten deels = 2 punten ad hoc / op verzoek = 1 punt nee = 0 punten
12	Welke conclusies worden aan de rapportages verbonden		1	geen =0 punten wel = 3 punten

F IdP systeem?

1	Welk systeem gebruikt u voor authenticatie en autorisatie in federatief identity management? Bijvoorbeeld: a. LDAP b. Active Directory c. Database (welke?)		0	altijd 0 punten (telt niet mee)
2	Welk pakket gebruikt u voor identity management?		1	geen of houtje touwtje = 0 punten anders 3 punten
3	Is dit systeem op een gestandaardiseerde manier aan te sluiten op federatief identity management?		2	ja = 3 punten nee = 0 punten
4	Welke standaard prefereert u? a. SAML b. A-select c. ADFS d. overig		1	geen = 0 punten standaard = 3 punten
5	Is uw IdP-systeem voldoende beschikbaar?		1	
6	Welke beschikbaarheid biedt u?		1	continu = 3 punten alleen 's nachts geen garantie = 2 punten business uren = 1 punt niet bepaald of lager = 0 punten

G Kwaliteit van de gegevens				
1	Zijn uw gegevens accuraat?		1	ja = 3 punten nee = 0 punten
2	Zijn uw gegevens volledig?		1	ja = 3 punten nee = 0 punten
3	Hoe snel worden uw gegevens aangepast na een wijzigings-verzoek?		1	real time = 3 punten (enkele minuten of minder) < 2 uur = 2 punten dagelijks = 1 punt anders 0 punten
4	Worden de gegevens geverifieerd tegen externe vertrouwde systemen? (denk aan IB-groep, GBA)		1	ja = 3 punten nee = 0 punten
H Implementatie van processen en procedures				
1	Zijn de processen en procedures duidelijk omschreven?		1	ja = 3 punten nee = 0 punten
2	Worden de diverse processen en procedures nageleefd?		1	ja = 3 punten deels = 2 punten nee = 0 punten
3	Is er toezicht op het naleven van de processen en procedures?		1	ja = 3 punten deels = 2 punten nee = 0 punten
4	Zijn de processen en de procedures bekend bij de juiste personen?		1	ja = 3 punten deels = 2 punten nee = 0 punten

I Veiligheid 				
1	Doet u aan 'awareness' rondom beveiliging en met name wachtwoorden?		1	ja = 3 punten nee = 0 punten
2	Is de veiligheid te verifiëren door een externe partij (audits)?		1	ja = 3 punten nee = 0 punten
3	Laat u wel eens intrusion tests uitvoeren op uw identity managementomgeving		1	ja = 3 punten nee = 0 punten
4	Is uw identity managementomgeving geclassificeerd?		1	ja = 3 punten nee = 0 punten
5	En zijn de bijbehorende maatregelen getroffen?		1	ja = 3 punten nee = 0 punten
6	Heeft u een doelstelling bepaald voor de identity managementvoorzieningen conform de WBP?		1	ja = 3 punten nee = 0 punten
7	Voldoet uw dienst aan de doelstelling (worden geen oneigenlijke gegevens geregistreerd)?		1	ja = 3 punten nee = 0 punten
8	Wat wordt er in logfiles opgeslagen, hoe lang en wie heeft er inzage?		1	ja = 3 punten nee = 0 punten