

sonicbee

Non-Human Identities

-

Van inzicht naar beheersbare digitale ketens

Opgesteld door:

Anass Choukrani | Business Consultant IAM
www.sonicbee.eu

Non-Human Identities: van technisch middel naar governance-vraagstuk

Inleiding

Om te begrijpen waarom non-human identities zo'n centrale rol spelen, helpt het om te kijken naar een alledaagse digitale handeling.

Een verkooporder wordt ingevoerd en vrijwel direct verwerkt. Voor de verkoper is dit een eenvoudige actie, maar op de achtergrond communiceren meerdere systemen met elkaar via API's en geautomatiseerde koppelingen. Elk systeem vertrouwt daarbij op het vorige: niet door de gebruiker te herkennen, maar door te verifiëren dat het aanleverende systeem daadwerkelijk is wie het zegt te zijn en bevoegd is om de order door te geven. In elke stap van de keten wordt dezelfde vraag gesteld: *komt deze aanvraag van het juiste systeem, en mag dit systeem dit doen?*

In moderne IT-landschappen verschuift verificatie steeds vaker van mensen naar systemen. Door de groei van geautomatiseerde en gekoppelde applicaties neemt het aantal non-human identities (NHI's) snel toe: digitale identiteiten die systemen zelfstandig toegang geven tot andere systemen en data. Hoewel deze identiteiten essentieel zijn voor continuïteit en schaalbaarheid, vallen zij in veel organisaties buiten bestaande identity- en governance-structuren. Het ontbreken van expliciet eigenaarschap, lifecycle-afspraken en risicosturing maakt NHI's daarmee tot een bestuurlijk en beheersmatig vraagstuk dat verder reikt dan techniek alleen.

Dit artikel laat zien hoe organisaties grip kunnen krijgen op het grotendeels onzichtbare landschap van non-human identities. Het beschrijft waarom NHI's nu relevant zijn, wat ze zijn, hoe ze ontstaan en hoe hun lifecycle eruitziet. Vervolgens wordt ingegaan op governance als vraagstuk van richting en eigenaarschap, en wordt een pragmatische, stapsgewijze aanpak geschetst die begint bij inzicht en positionering.

De centrale boodschap daarbij is eenvoudig: grip op non-human identities begint met focus. Start met een apart NHI-traject in korte sprints (6–8 weken), met een assessment op de huidige situatie gericht op inzicht in wat er is, waarom het bestaat en wie ervoor verantwoordelijk is. Een pragmatische aanpak die de basis vormt voor een onderbouwd vervolgplan, zonder direct te vervallen in tooling of een zwaar programma.

Inhoudsopgave

Non-Human Identities: van technisch middel naar governance-vraagstuk	2
<i>Inleiding</i>	<i>2</i>
1. Waarom NHI's nu relevant zijn	4
2. Wat NHI's zijn (en niet)	4
3. Ontstaan van NHI's	4
4. Lifecycle van NHI's	5
5. Governance van NHI's	5
6. Waar te beginnen	6
1. <i>Breng het NHI-landschap in kaart.....</i>	<i>6</i>
2. <i>Ontwikkel een gedeeld begrippenkader en positionering</i>	<i>6</i>
3. <i>Formuleer een concreet doel en ambitie voor NHI-beheer</i>	<i>6</i>
4. <i>Stel uitgangspunten vast voor eigenaarschap, risico en lifecycle</i>	<i>6</i>
<i>Van inzicht naar gerichte vervolgstappen</i>	<i>7</i>
7. Drie herkenbare situaties.....	7
A. <i>Een kleine wijziging met grote ketenimpact.....</i>	<i>7</i>
B. <i>Tooling ingezet, maar het risico blijft bestaan</i>	<i>8</i>
C. <i>Van incident naar beheersing.....</i>	<i>8</i>
NHI's beheersen is een ontwikkelpad	9

1. Waarom NHI's nu relevant zijn

Het belang van non-human identities is de afgelopen jaren sterk toegenomen. Door cloudadoptie, DevOps-werkwijzen, ketenintegraties en automatisering groeit het aantal identiteiten dat zelfstandig systemen en data benadert exponentieel. In veel omgevingen zijn NHI's inmiddels vele malen talrijker dan menselijke identiteiten.

Deze groei verloopt vaak impliciet: NHI's ontstaan als noodzakelijk technisch middel om processen werkend te krijgen, maar zonder dat daar expliciet beleid of governance op wordt ingericht. Hierdoor blijven identiteiten en bijbehorende secrets regelmatig langer actief dan nodig (NHI1), of krijgen zij meer rechten dan functioneel vereist (NHI5/NHI9). In combinatie met het hergebruik van credentials of het ontbreken van duidelijke eigenschap ontstaat een structureel spanningsveld tussen snelheid en controle. Wat begint als een praktische oplossing, kan zich daardoor ontwikkelen tot een blinde vlek binnen het security- en risicomanagement van de organisatie.

2. Wat NHI's zijn (en niet)

Non-human identities zijn digitale identiteiten die door systemen, applicaties, scripts of processen worden gebruikt om zich te authenticeren en toegang te verkrijgen tot andere systemen of gegevens. Het gaat hierbij onder meer om service accounts, applicatie-identiteiten, API-sleutels, certificaten en vergelijkbare vormen van machine-authenticatie die nodig zijn voor geautomatiseerde interacties.

Minstens zo belangrijk is wat non-human identities *niet* zijn. Het zijn geen gebruikersaccounts en geen menselijke identiteiten, en zij passen niet vanzelfsprekend binnen HR-gedreven processen zoals joiner-mover-leaver. Daarnaast zijn NHI's niet gelijk te stellen aan losse credentials of tokens; dergelijke middelen vormen slechts technische representaties van een onderliggende identiteit. Juist dit onderscheid helpt om non-human identities te begrijpen als een eigen categorie binnen het identity-domein, met kenmerken die verschillen van menselijke identiteiten.

3. Ontstaan van NHI's

Non-human identities ontstaan zelden vanuit een bewuste governance-beslissing. In de praktijk zijn ze meestal het resultaat van projecten en technische keuzes: het koppelen van applicaties, het automatiseren van rapportages, het inrichten van CI/CD-pipelines of het ontsluiten van data via API's.

Deze identiteiten worden doorgaans aangemaakt door ontwikkelteams, beheerders of externe leveranciers, met de nadruk op functionaliteit en doorlooptijd. Expliciet eigenaarschap, een vastgestelde gebruiksduur of structurele controle ontbreken daarbij vaak. Hierdoor blijven NHI's bestaan nadat hun oorspronkelijke doel is vervallen, of groeien hun rechten mee met veranderende omgevingen zonder herbeoordeling.

4. Lifecycle van NHI's

Net als menselijke identiteiten kennen non-human identities een lifecycle: ze worden aangemaakt, aangepast, gebruikt en zouden uiteindelijk ook weer moeten worden ingetrokken. In tegenstelling tot menselijke identiteiten is deze lifecycle echter zelden expliciet ingericht. In de praktijk ontbreekt vaak een gedeelde manier om deze stappen te benoemen en te structureren, vergelijkbaar met hoe bij menselijke identiteiten het joiner–mover–leaver-model wordt toegepast. Voor non-human identities kan een lifecycle-benadering zoals Create, Adjust en Remove (CAR) helpen om dit proces inzichtelijk en bestuurbaar te maken.

Waar de lifecycle van menselijke identiteiten is ingebed in HR-gedreven governance-structuren, wordt de lifecycle van non-human identities veelal ingericht via change- en beheerprocessen, wat vraagt om expliciete afstemming binnen identity governance. Aandacht voor het aanpassen van rechten, het roteren van credentials of het tijdig decommissionen ontbreekt regelmatig. Dit leidt tot zogenoemde *orphan identities*, langdurig geldige secrets en moeilijk traceerbare toegang, wat het risico op misbruik aanzienlijk vergroot. Inzicht in en beheersing van de NHI-lifecycle vormt daarmee een cruciale randvoorwaarde voor volwassen identity governance.

5. Governance van NHI's

Governance rondom non-human identities betekent dat organisaties expliciet vastleggen welke identiteiten bestaan, waarvoor zij worden ingezet en wie daarvoor verantwoordelijk is. Dit is noodzakelijk omdat NHI's vaak brede technische rechten hebben en grotendeels buiten reguliere identity- en access-controles opereren. Succesvolle NHI-governance is zichtbaar wanneer een organisatie inzicht heeft in welke NHI's actief zijn, welk doel zij dienen, wie het eigenaarschap draagt en welke risico's eraan verbonden zijn.

Een effectieve governance-aanpak begint niet bij tooling, maar bij richting en focus. In een eerste plateau ligt de nadruk op het creëren van overzicht en positionering. Dit gebeurt via een apart NHI-traject in korte sprints, gestart met een beknopt assessment van de huidige situatie. Binnen deze startfase worden stapsgewijs de volgende elementen uitgewerkt:

- het ontwikkelen van een gedeeld begrippenkader en een duidelijke positionering van NHI's binnen de organisatie;
- het formuleren van een concreet doel en ambitie voor NHI-beheer;
- het vaststellen van uitgangspunten voor eigenaarschap, risicosturing en lifecycle-beheer.

Het resultaat is een onderbouwd en gedragen vertrekpunt: helder inzicht in het NHI-landschap en een concreet kader voor vervolgstappen. Deze gefaseerde aanpak volgt de wet van Liebig: de mate van beheersing wordt bepaald door de zwakste schakel. Zolang fundamentele elementen zoals inzicht, eigenaarschap of lifecycle-afspraken ontbreken, zullen verdere investeringen in processen of tooling het effect beperken. In de volgende paragraaf wordt daarom concreter ingegaan op waar te beginnen.

6. Waar te beginnen

Grip op non-human identities begint met focus. In de praktijk betekent dit het starten van een afgebakend NHI-traject in korte sprints (6–8 weken), met als doel niet om direct technische oplossingen te implementeren, maar om richting, overzicht en bestuurbaarheid te creëren. Dit traject vormt de concrete uitwerking van het eerste plateau uit de governance-aanpak.

1. Breng het NHI-landschap in kaart

Het traject start met een beknopt assessment van de huidige situatie, gericht op drie kernvragen: **welke non-human identities bestaan er, waarom bestaan ze en wie is ervoor verantwoordelijk?** Deze eerste inventarisatie brengt NHI's in kaart binnen applicaties, cloudomgevingen, integraties en automatisering, inclusief hun functionele rol en globale risicokarakteristieken. Volledigheid is hierbij geen vereiste; het doel is voldoende inzicht om patronen, afhankelijkheden en blinde vlekken zichtbaar te maken.

2. Ontwikkel een gedeeld begrippenkader en positionering

Op basis van dit overzicht wordt eerst een gedeeld begrippenkader ontwikkeld. In veel organisaties bestaan uiteenlopende interpretaties van wat onder non-human identities valt: van service accounts en API-sleutels tot certificaten, cloud-rollen en automatiseringsaccounts. Door expliciet vast te stellen welke typen NHI's relevant zijn, hoe zij zich verhouden tot bestaande IAM-concepten en waar zij organisatorisch worden gepositioneerd, ontstaat een gezamenlijk referentiekader. Dit maakt NHI's zichtbaar als een eigen identiteitscategorie, met andere kenmerken en risico's dan menselijke identiteiten.

3. Formuleer een concreet doel en ambitie voor NHI-beheer

Vervolgens wordt bepaald wat de organisatie met NHI-beheer wil bereiken. Niet in abstracte termen, maar vertaald naar een realistische ambitie: gaat het primair om risicoreductie, audit-volwassenheid, betere beheersbaarheid of het veilig ondersteunen van verdere automatisering? Door dit doel expliciet te maken, ontstaat focus en samenhang. Het voorkomt dat het traject verzandt in losse inventarisaties of geïsoleerde technische verbeteringen zonder duidelijke richting.

4. Stel uitgangspunten vast voor eigenaarschap, risico en lifecycle

Pas daarna worden de uitgangspunten vastgesteld voor hoe met NHI's wordt omgegaan. Dit betreft onder meer wie eindverantwoordelijk is voor een NHI, hoe lifecycle-momenten zoals aanmaken, wijzigen en intrekken worden herkend en gestuurd, en welke risicofactoren bepalend zijn voor prioritering. Daarbij gaat het bijvoorbeeld om brede rechten, langlevende of hergebruikte credentials en kritieke procesafhankelijkheden. Deze uitgangspunten maken het mogelijk om NHI's niet alleen te inventariseren, maar ook te duiden: welke categorieën vragen als eerste aandacht en waarom?

Van inzicht naar gerichte vervolgstappen

Het resultaat van dit eerste traject is geen technische oplossing, maar een onderbouwd vertrekpunt: een gedeeld begrippenkader, expliciet eigenaarschap en inzicht in waar de grootste risico's en verbeterkansen liggen. Op basis hiervan kan een realistisch vervolgplan worden opgesteld, waarin vervolgstappen, zoals verdere life-cycle-inrichting, procesafspraken en pas daarna eventuele tooling, logisch en beheersbaar worden geprioriteerd. Niet door te streven naar perfectie, maar vanuit het besef dat elke gerichte stap vooruit daadwerkelijk grip oplevert.

7. Drie herkenbare situaties

Om dit concreet te maken volgen hieronder drie herkenbare praktijksituaties. Ze laten zien waar het misgaat, waarom techniek alleen onvoldoende is en wat een effectievere aanpak is.

A. Een kleine wijziging met grote ketenimpact

Zoals in de inleiding beschreven, vertrouwen moderne orderketens op systeemidentiteiten om transacties automatisch te verwerken.

In één van die systemen wordt een serviceaccount gebruikt met een statische API-sleutel en brede rechten, ooit aangemaakt “voor de koppeling”. Het account wordt door meerdere integraties hergebruikt en heeft geen expliciet eigenaarschap.

Wanneer een ontwikkelaar een bestaande koppeling hergebruikt voor een nieuw project, blijft dezelfde NHI actief omdat deze al werkt. Door de ruime rechten krijgt de aangepaste applicatie onbedoeld toegang buiten de oorspronkelijke scope. Orders worden automatisch geaccepteerd met foutieve parameters, wat leidt tot vervuilde data en herstelwerk achteraf.

Er is niets gehackt en de wijziging is correct doorgevoerd. Het probleem zit in de NHI zelf: een over-privileged, statische identiteit zonder duidelijke positionering, eigenaarschap of herbeoordeling. Niet techniek faalt hier, maar het ontbreken van inzicht en governance, waardoor een kleine interne wijziging een groot keteneffect krijgt.

B. Tooling ingezet, maar het risico blijft bestaan

De organisatie implementeert NHI-tooling om grip te krijgen op serviceaccounts en secrets. Identiteiten worden geregistreerd, credentials automatisch geroteerd en gebruik wordt gemonitord. Technisch lijkt alles onder controle.

Toch ontstaat een incident wanneer een bestaande NHI wordt hergebruikt voor een nieuwe ketenintegratie. De tooling staat dit toe: rechten zijn geldig, policies worden gevolgd en rotatie werkt correct. Wat ontbreekt is context. Er is nooit vastgelegd waarvoor deze NHI bedoeld is, welke procesgrenzen gelden en wie verantwoordelijk is voor dat gebruik.

Enkele weken later blijkt dat data uit verschillende domeinen onbedoeld wordt gecombineerd. Niet door falende techniek, maar doordat één technisch correcte NHI meerdere bedrijfsprocessen bedient. Security ziet geen overtreding, maar business en compliance zien een probleem.

De conclusie is helder: tooling beheert middelen, maar geen betekenis. Zonder expliciete positionering, eigenaarschap en gebruiksafspraken blijft het onderliggende risico bestaan, hoe volwassen de tooling ook is.

C. Van incident naar beheersing

Na de problemen uit voorbeeld A en B start de organisatie een apart NHI-traject in korte sprints. Eerst wordt inzicht gecreëerd: welke non-human identities zijn betrokken bij het orderproces, waarvoor worden ze gebruikt en wie is verantwoordelijk.

Dit maakt zichtbaar dat meerdere applicaties dezelfde NHI's delen en dat eigenaarschap ontbreekt. Op basis daarvan worden gerichte maatregelen genomen: kritieke NHI's krijgen een eigenaar, rechten worden teruggebracht tot de functionele noodzaak en gebruik in meerdere contexten wordt expliciet begrensd.

Enkele maanden later is het proces niet perfect, maar wel beheersbaar. Wijzigingen leiden niet langer tot onverwachte kettingreacties en incidenten zijn sneller te herleiden. Niet door meer tooling, maar door gerichte focus, inzicht en duidelijke verantwoordelijkheid.

NHI's beheersen is een ontwikkelpad

Non-human identities zijn geen technisch randverschijnsel, maar een structureel governance-vraagstuk. Ze dragen bedrijfskritische processen, beschikken vaak over vergaande rechten en opereren op schaal, terwijl eigenaarschap, context en lifecycle-afspraken in veel organisaties ontbreken. Juist die combinatie maakt NHI's tot een onderschat risico binnen security, compliance en operationele continuïteit.

Dit artikel laat zien dat grip op NHI's niet begint bij tooling, maar bij focus en richting. Door NHI's expliciet te positioneren als een eigen identiteitscategorie, met duidelijke doelen, eigenaarschap en uitgangspunten, ontstaat overzicht en bestuurbaarheid. Pas vanuit die basis kunnen processen worden aangescherpt en technische maatregelen effectief worden ingezet.

De voorbeelden maken duidelijk wat er gebeurt als die basis ontbreekt: kleine interne wijzigingen krijgen een disproportioneel effect, tooling mist context en incidenten zijn moeilijk te duiden. Tegelijk laten ze zien dat een pragmatische, gefaseerde aanpak wél werkt. Niet door perfectie na te streven, maar door stap voor stap inzicht te vergroten en verantwoordelijkheid expliciet te maken.

Grip op non-human identities is daarmee geen eindproject, maar een ontwikkel-pad. Organisaties die dit pad bewust bewandelen, leggen een solide fundament voor veilige automatisering, schaalbaarheid en duurzame digitale groei.