

WHITEPAPER

De voordelen van een **Physical Identity & Access Management (PIAM)-platform als Software as a Service**

Hoge beveiliging. Snelle uitrol.

Altijd up-to-date.

Inhoudsopgave

Inleiding	1
1. Wat is Physical Identity & Access Management?	1
2. Waarom organisaties SaaS inzetten	2
2.1 Wat er met SaaS verandert	2
3. Het PIAM-SaaS-aanbod van ID-ware	3
3.1 De ID-ware PIAM Suite	3
3.2 De voordelen van de ID-ware PIAM Suite als SaaS	3
4. Het Platform Engineering Team (PET)	4
4.1 Vijf kerngebieden	5
5. Veelgehoorde bezwaren — en onze antwoorden daarop	6
6. Totale gebruikskosten: on-premises vs. SaaS	7
6.1 De verborgen kosten van een on-premises installatie	7
6.2 On-premises en SaaS vergeleken	8
6.3 Bedrijfsprofielen en totale gebruikskosten	9
7. Sectoren die de SaaS-oplossing van ID-ware inzetten	11
8. Conclusie	11

Inleiding

Organisaties in alle sectoren staan voor dezelfde uitdaging: het beheren van fysieke identiteiten (medewerkers, dienstverleners, bezoekers) en hun toegang tot gebouwen, beveiligde zones en gevoelige locaties. Traditioneel vroeg dat om forse investeringen in on-premises software en om eigen infrastructuurteams voor beheer en onderhoud.

De inzet van Software as a Service (SaaS) verandert dit fundamenteel. De verantwoordelijkheid voor de infrastructuur ligt bij de gespecialiseerde leverancier: enterprisefunctionaliteit zonder enterprise-IT-inspanning. Toegepast op Physical Identity & Access Management (PIAM) worden de voordelen nog duidelijker: snellere uitrol, lagere totale gebruikskosten (Total Cost of Ownership/TCO), betere ondersteuning bij compliance en schaalbaarheid.

Dit whitepaper laat zien waarom PIAM als SaaS strategisch verstandig is, en beschrijft hoe de PIAM Suite van ID-ware organisaties van elke omvang toegang geeft tot een enterpriseplatform, zonder de klassieke investeringslast. Waar SaaS niet is toegestaan, is het platform ook beschikbaar als private cloud, managed cloud hosting of on-premises installatie.

1. Wat is Physical Identity & Access Management?

Physical Identity & Access Management (PIAM) verbindt het beheer van persoonsidentiteiten met de sturing van hun toegang tot gebouwen en beveiligde zones. Een PIAM-platform is de leidende gegevensbron voor wie zich waar mag bevinden en onder welke voorwaarden.



Credential Management

Volledige levenscyclus van fysieke credentials – van ontwerp en personalisatie tot uitgifte en blokkering.



Access Management

Workflowgestuurd beheer van toegangsrechten over alle locaties van een organisatie heen.



Visitor Management

Geautomatiseerde bezoekersregistratie, vooraanmelding, identiteitscontrole en check-in- en check-outprocessen.



Contractor Management

Onboarding en toegangsbeheer voor externe firma's, inclusief controle van certificaten en automatisch intrekken van toegangsrechten na afloop van het contract.



User Self-Service & Photon

Self-Service-portaal waarmee medewerkers credential gegevens, toegangsaanvragen en portretfoto's zelf beheren.



Integraties

Connectoren met HR-systemen en directoryservices, toegangscontrolesystemen en systemen van derden zoals parkeer-, kluisjes- of betaalsystemen.

Zonder één samenhangend PIAM-platform werken organisaties vaak met een lappendeken van losstaande eilandoplossingen. Dat leidt tot hiaten in compliance, veel administratieve last en vermijdbare beveiligingsrisico's.

2. Waarom organisaties SaaS inzetten

Een Software-as-a-Service (SaaS)-oplossing draait bij een leverancier in de cloud en wordt op abonnementsbasis afgenomen, in plaats van gekocht, on-premises geïnstalleerd en onderhouden. In het afgelopen decennium is dit model de standaard geworden voor bedrijfssoftware.

Belangrijkste voordeel



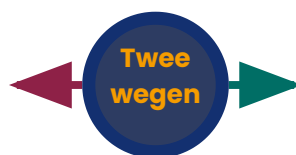
PIAM op enterpriseniveau, zonder enterprise-IT-inspanning.

2.1 WAT ER MET SAAS VERANDERT

De overstap van on-premises naar managed SaaS verandert de kostenstructuur, het risicoprofiel en de operationele inspanning fundamenteel. De verantwoordelijkheid voor infrastructuur, beschikbaarheid en platformbeveiliging gaat over naar een leverancier wiens kernactiviteit het beheer van dat platform is. De organisatie houdt de volledige controle over haar processen, rollen en gegevens. De volgende vergelijking laat de verschillen zien.

ON-PREMISES

- Hoge initiële investering
- Eigen IT-team nodig
- Risico- en compliance-verantwoordelijkheid intern
- Vertraagde upgrades
- Risico bij capaciteitsplanning
- Noodherstel in eigen beheer
- Compliance in eigen beheer



Complexiteit groeit
vs.
Eenvoud neemt toe

MANAGED SAAS

- Planbare abonnementskosten
- Platformteam inbegrepen
- Risico bij de leverancier
- Altijd up-to-date
- Ingebouwde redundantie
- Flexibel schalen
- Ondersteunt compliance

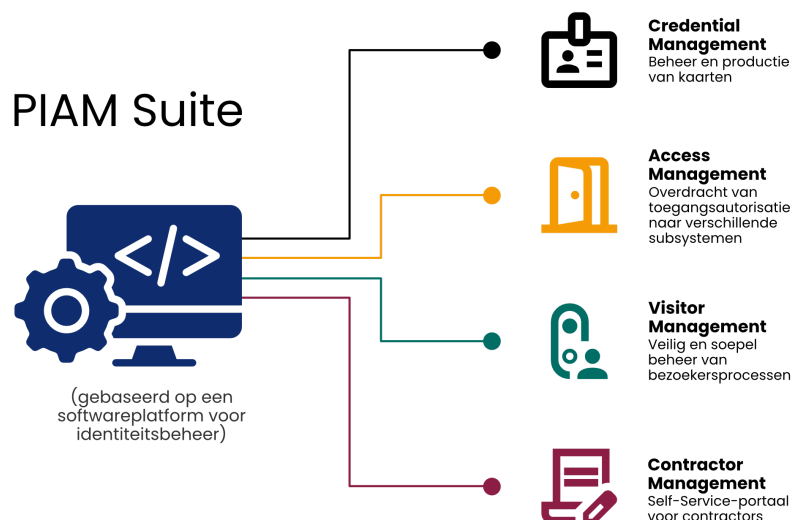
KERNBOODSCHAP

Organisaties die een PIAM-platform als SaaS inzetten, verlagen niet alleen hun operationele kosten. Ze **dichten tegelijk een aanzienlijk beveiligings- en verantwoordingsgat** dat klassieke on-premises installaties open laten.

3. Het PIAM-SaaS-aanbod van ID-ware

ID-ware is een gespecialiseerde leverancier van Physical Identity & Access Management (PIAM)-oplossingen met ruim 20 jaar ervaring. De oplossingen worden ingezet door organisaties in Europa en daarbuiten. De ID-ware PIAM Suite als SaaS helpt organisaties het beheer van fysieke identiteiten en toegangsrechten te vereenvooudigen, en verlaagt tegelijk kosten, complexiteit en compliancerisico's.

3.1 DE ID-WARE PIAM SUITE



3.2 DE VOORDELEN VAN DE ID-WARE PIAM SUITE ALS SAAS

Als SaaS-oplossing biedt de PIAM Suite beheer van fysieke identiteiten en toegangsrechten op enterpriseniveau, zonder eigen infrastructuur. ID-ware neemt de verantwoordelijkheid voor hosting, beschikbaarheid, updates en de beveiliging van het platform.

- Hoge beveiliging**
Hosting in Europa: gegevens verlaten gecertificeerde EU-datacenters niet
- Hoge beschikbaarheid**
99,9 % beschikbaarheid, ingebouwde redundantie en automatische failover
- Regelmatige updates**
Alle patches en releases worden automatisch door ID-ware uitgerold
- Snelle uitrol**
Activering en oplevering van de omgeving op dezelfde dag in het public-SaaS-model
- Aanpasbaarheid**
Ruim configureerbare functionaliteit, passend bij de eigen processen
- Ondersteuning bij compliance**
Ondersteunt bij het voldoen aan verplichtingen uit NIS2, DORA, AVG en ISO 27001

4. Het Platform Engineering Team (PET)

Uw infrastructuur.
**Onze
verantwoordelijkheid.**

Achter het SaaS-aanbod van ID-ware staat een eigen Platform Engineering Team (PET): ervaren platform engineers, cloud architects en cloud engineers die de onderliggende cloudinfrastructuur ontwerpen, bouwen en beheren.



Het takenpakket van het PET omvat vijf kerngebieden

Elk gebied wordt volledig door ID-ware verzorgd, van het inrichten van de infrastructuur tot het bewaken van compliance. De organisatie kan zich volledig richten op het gebruik van de PIAM Suite.

WAT DAT CONCREET BETEKENT



Altijd up-to-date

Elke update en elke beveiligingspatch wordt automatisch door ID-ware uitgerold. De omgeving draait altijd op de actuele versie, zonder eigen inspanning.



Schaalt mee

De infrastructuur groeit automatisch mee met de behoefte van de organisatie: geen capaciteitsplanning, geen risico op overdimensionering, geen knelpunten.



Ontworpen op continuïteit

Zelfherstellende architectuur en automatische failover houden het PIAM-platform continu beschikbaar, aangevuld met doorlopende bewaking door het team van ID-ware.

Geen infrastructuurlast: de eigen teams richten zich volledig op het gebruik van de PIAM Suite, in plaats van servers onderhouden, patches uitrollen of capaciteit plannen.

4.1 HET PLATFORM ENGINEERING TEAM (PET) — VIJF KERNGEBIEDEN

De vijf kerngebieden van het PET grijpen in elkaar. Elk gebied is onmisbaar voor een platform dat veilig, beschikbaar en altijd actueel is en dat ondersteunt bij het voldoen aan regelgeving. Alle gebieden worden volledig door ID-ware verzorgd.



5. Veelgehoorde bezwaren – en onze antwoorden daarop

Organisaties die een overstap naar managed SaaS overwegen, stellen meestal dezelfde vragen. Hier de antwoorden.

Zoals de antwoorden hierna laten zien, **houden de gebruikelijke bezwaren tegen SaaS bij nadere beschouwing geen stand** – in de meeste gevallen is het managed-SaaS-model op elk van deze punten voordeliger dan een zelfbeheerde oplossing.



Is een SaaS-platform aan te passen aan eigen processen?

De ID-ware PIAM Suite is **uitgebreid configureerbaar**. De modulaire architectuur stelt organisaties in staat **alleen de functies te gebruiken die zij nodig hebben** en die af te stemmen op de eigen processen – niet andersom.



Hoe zit het met de gegevensbeveiliging in de cloud?

Alle gegevens staan in **Europees gecertificeerde datacenters**, conform de eisen van de AVG aan de opslaglocatie. Het platform omvat **centraal beveiligingsbeheer inclusief infrastructuurbeveiliging**. ID-ware is **gecertificeerd volgens ISO 9001 en ISO 27001** en is TISAX-deelnemer.



Leidt een abonnement niet tot afhankelijkheid?

ID-ware biedt **flexibele contractduren** die met de organisatie meegroeien. Schaalbaarheid zit zowel in de oplossing als in het prijsmodel – de **omvang is uit te breiden of aan te passen** als de eisen veranderen, zonder starre meerjarige verplichtingen.



Wat gebeurt er bij groei of veranderende eisen?

De ID-ware PIAM Suite **schaalt elastisch** mee met de organisatie. Nieuwe locaties, gebruikers of modules vragen **geen wijzigingen aan de eigen infrastructuur** – het PET van ID-ware verzorgt provisioning, capaciteit en uitrol. Er wordt alleen betaald voor het werkelijke gebruik.



Is SaaS geschikt voor grote, professionele organisaties?

SaaS is **wereldwijd het dominante softwaremodel voor ondernemingen**. De meerderheid van de Fortune 500-bedrijven draait kritieke processen op SaaS. De ID-ware PIAM Suite als SaaS is geschikt voor organisaties van elke omvang, maar is **ontwikkeld voor complexe omgevingen**.



Is migratie vanaf een bestaand on-premises systeem bewerkelijk?

De **gestructureerde onboarding** van ID-ware zorgt voor een soepele overgang vanaf elk bestaand systeem. Omgevingen in het **public-SaaS-model staan dezelfde dag klaar**, en specialisten van ID-ware begeleiden de migratie van datamapping tot go-live – zo blijft **de verstoring gedurende het hele traject minimaal**.

6. Totale gebruikskosten: on-premises vs. SaaS

Een gestructureerde analyse van de totale gebruikskosten (Total Cost of Ownership/TCO) laat het werkelijke financiële en operationele resultaat zien bij de vergelijking tussen eigen beheer en SaaS. Op alle gebieden (infrastructuur, personeel, compliance en schaalbaarheid) biedt het SaaS-model consistent minder risico, lagere kosten en eenvoudiger beheer.

6.1 DE VERBORGEN KOSTEN VAN EEN ON-PREMISES INSTALLATIE

De licentiekosten zijn slechts het topje van de ijsberg

De TCO van een on-premises installatie overtreft de oorspronkelijke ramingen stelselmatig. Doorslaggevend zijn de verborgen kosten.

3-5x

zo hoge werkelijke TCO ten opzichte van de licentiekosten



MEER DAN ALLEEN DIRECTE KOSTEN

Diverse factoren staan op geen enkele factuur, maar bepalen wel wat een installatie gedurende haar levensduur werkelijk kost.

Innovatiesnelheid

In eigen beheer moet elke update intern worden getest en uitgerold. Bij SaaS zijn nieuwe functies direct na hun release beschikbaar.

Service niveaus

Een zelfbeheerd platform vraagt intern gedefinieerde en intern bemenste serviceniveaus. SaaS wordt geleverd op basis van een overeengekomen Service Level Agreement (SLA), d.w.z. inclusief onderhoud.

Financiële voorspelbaarheid

On-premises combineert investeringsuitgaven met schommelende beheerkosten. SaaS is één enkele, voorspelbare exploitatiepost.

Business continuity

Eigen beheer vraagt een eigen noodherstelplan. Failover over meerdere beschikbaarheidszones maakt deel uit van het SaaS-platform.

6.2 ON-PREMISES EN SAAS VERGELEKEN

Gebied	On-premises	ID-ware SaaS
Infrastructuur	Investering in hardware en/of datacentercapaciteit nodig.	Infrastructuur is inbegrepen in de SaaS-prijs. Geen aparte investering nodig.
Beheer & personeel	Eigen intern IT-team nodig voor monitoring, back-up, patching en hoge beschikbaarheid.	ID-ware verzorgt het volledige beheer, updates, monitoring en beveiliging.
Beveiliging & compliance	De organisatie is als enige verantwoordelijk voor AVG, certificeringen en penetratietests.	ID-ware beschikt over de relevante certificeringen volgens ISO 27001 en ISO 9001; centrale beveiliging en audit trails zijn standaard.
Schaalbaarheid	Extra capaciteit vraagt investeringen. Risico op over- of onderdimensionering.	Schalen op afroep. De kosten groeien lineair mee met het gebruik; het risico op overdimensionering vervalt.
Eindoordeel	Zinvol wanneer eisen aan datasoevereiniteit, intern cloudbeleid of een omvangrijke bestaande IT-infrastructuur dat vragen — een model dat ID-ware volledig ondersteunt.	Voordeliger, met minder risico, lagere vaste kosten en betere schaalbaarheid voor de meeste organisaties.

99,9 %

platformbeschikbaarheid voor elke door ID-ware geleverde SaaS-omgeving

1 dag

na contractondertekening duurt het opleveren van de omgeving in het public-SaaS-model

TCO-conclusie: de verstandigste keuze voor PIAM

SaaS-hosting voorkomt investeringsuitgaven, verlegt het operationele risico naar ID-ware, garandeert contractueel overeengekomen SLA's en biedt doorlopende toegang tot de nieuwste functies, tegen voorspelbare abonnementskosten.

Voor PIAM-oplossingen waarbij compliance, beveiliging en beschikbaarheid onmisbaar zijn, is dit model niet alleen het gemakkelijkst, maar ook de verstandigste keuze.

6.3 BEDRIJFSPROFIELEN EN TOTALE GEBRUIKSKOSTEN

SaaS of on-premises? Die vraag wordt niet beslist door de omvang van een organisatie, maar door **de aard van de investering** en door de manier waarop een organisatie de verantwoordelijkheid voor beheer en beveiliging wil dragen.

On-premises betekent een aanzienlijke initiële inspanning voor hardware, licenties en inrichting, daarna intern personeel voor de doorlopende kosten en vervangingsinvesteringen zodra hardware of versies het einde van hun levensduur bereiken. De verplichting wordt jaren aangegaan voordat het voordeel volledig wordt gerealiseerd.

SaaS zet dit om in een vast terugkerend bedrag — zonder teams voor onderhoud, patching of updates, en zonder kapitaal dat vastzit in infrastructuur.

Beveiliging hoort in dezelfde rekensom thuis. Een managed-SaaS-omgeving is doorgaans **veiliger dan een zelfbeheerde installatie**. In plaats van te wachten op een intern onderhoudsvenster werken patches en beveiligingsupdates direct door, en het platform wordt centraal bewaakt. De drie bedrijfsprofielen hierna laten zien hoe dit bij verschillende schaalgroottes uitwerkt op de totale gebruikskosten.

BEDRIJFSPROFIEL A

Kleinere en middelgrote organisaties

- Geen platformteam nodig: beheer, patching en back-ups worden verzorgd door ID-ware
- De afhankelijkheid van één of twee interne specialisten vervalt
- Enterprisebeschikbaarheid zonder enterprise-IT
- Voorspelbare doorlopende kosten in plaats van een initiële investering voor een on-premises installatie

Conclusie: SaaS is de juiste keuze.

BEDRIJFSPROFIEL B

Grotere organisaties met gevestigde IT-processen

- Specialisten blijven op vakinhoudelijke projecten in plaats van het platform te onderhouden
- Serviceniveaus staan in het contract en hoeven niet intern te worden ingevuld
- Het operationele risico ligt bij ID-ware, niet bij het eigen team
- Extra gebruikers en locaties zijn te realiseren zonder nieuwe investeringscyclus

Conclusie: SaaS overtuigt op opportuiniteitskosten en risico-overdracht.

BEDRIJFSPROFIEL C

Organisaties met veel locaties en concernstructuren

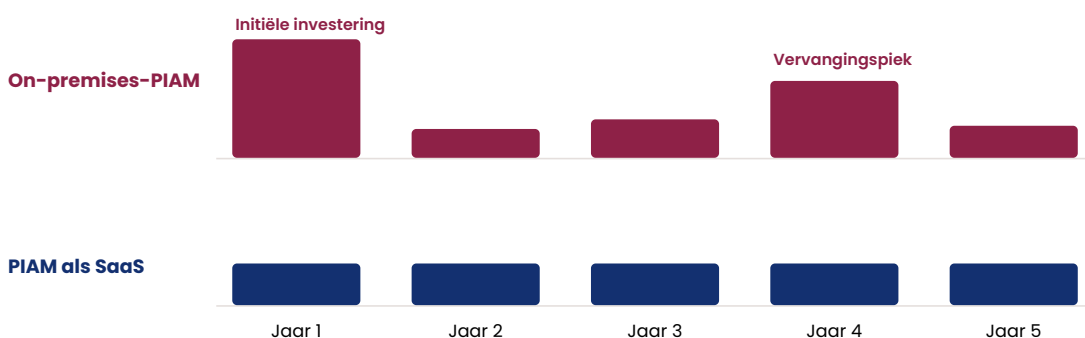
- Geen lokale IT-aanwezigheid op de afzonderlijke locaties nodig
- Een uniform beveiligingsniveau en consistente rapportage ondersteunen de auditgereedheid op alle locaties
- Een nieuwe locatie of overname is slechts een configuratiestap in plaats van een nieuw project
- De capaciteit voor nieuwe locaties en gebruikers levert ID-ware, zonder inkoop of doorlooptijd

Conclusie: SaaS schaalt moeiteloos mee, waar de groep ook groeit.

De vergelijking is structureel van aard: zij beschrijft hoe kosten en inspanning zich verdelen, niet wat een concrete configuratie kost. Op die basis zijn de drie bedrijfsprofielen aan de hand van de onderstaande punten praktisch te beoordelen. In de meeste organisaties gelden meerdere punten tegelijk, en juist die combinatie geeft de doorslag.

DE AARD VAN DE INVESTERING

On-premises concentreert de uitgaven in één grote initiële investering en latere vervangingspieken. SaaS biedt dezelfde functionaliteit, maar tegen een voorspelbaar, terugkerend bedrag.



Schematische weergave van de kostenverdeling over de tijd. Geen absolute bedragen.

HOE SAAS ZICH TERUGBETAALT

- De investering is een **vast terugkerend bedrag** in plaats van een grote initiële uitgave.
- Nieuwe releases **gaan snel in productie**, zonder dat elke keer een intern uitrolproject nodig is.
- Een **eigen team voor platformbeheer** is niet nodig.
- Beschikbaarheid en herstel zijn **contractueel gegarandeerd** en hoeven niet intern te worden gerealiseerd.
- Voor onderhoud, patching en updates hoeft **geen interne capaciteit te worden opgebouwd**.

LET OP: ALS SAAS GEEN OPTIE IS

In sommige domeinen, bijvoorbeeld de publieke sector, kritieke infrastructuur of andere hoogrisico-omgevingen, kunnen intern beleid of sectorregels een ander implementatiemodel vereisen. ID-ware biedt ook **private cloud, managed cloud hosting en on-premises beheer** aan, telkens met dezelfde functionaliteit van de software en dezelfde supportorganisatie.

Organisaties die nu een on-premises installatie gebruiken, kunnen op elk moment overstappen naar een SaaS-model. De overgang wordt zorgvuldig en in nauw overleg met de betrokken teams gepland en doorlopend begeleid door ID-ware.

7. Sectoren die de SaaS-oplossing van ID-ware inzetten

De PIAM Suite van ID-ware als SaaS wordt ingezet in sectoren die fysieke toegang op grote schaal beheren. Hierna volgen typische toepassingsvoorbeelden: elke sector brengt eigen eisen mee – alle worden gedekt door hetzelfde platform.



Onderwijs & Universiteiten

Beheer van grote, diverse groepen studenten, medewerkers en bezoekers over meerdere campussen, met efficiënte registratie bij massale inschrijving.



Industrie & Productie

Sturing van de toegang tot productiegebieden en gevarenczones, inclusief bezoekers- en aannemersmanagement. Ondersteuning bij het voldoen aan eisen uit ISO, AVG en NIS2.



Publieke sector & Kritieke infrastructuur

Ondersteuning van strenge eisen aan beveiliging en datasoevereiniteit door Europese single-tenant hosting in de private cloud (is dat geen optie, dan draait de PIAM Suite van ID-ware ook on-premises).



Lucht- & ruimtevaart

Streng afgebakende toegang tot verboden zones, integratie van screeningsprocessen voor personeel en sluitende controleerbaarheid, zoals vereist voor veiligheidsonderzoeken.



Financiële sector

Ondersteuning van de DORA-weerbaarheidseisen en sectorspecifieke auditeisen ten aanzien van fysieke toegang.



Gezondheidszorg & Medisch

Beheer van de toegang tot patiëntgebieden, geneesmiddelenopslag en onderzoeksfaciliteiten met sluitende audit trails.

8. Conclusie

Physical Identity & Access Management (PIAM) is een bepalende factor voor beveiliging, operationele efficiëntie en het naleven van wettelijke voorschriften. Toch werken veel organisaties nog met verouderde on-premises tools die onvoldoende bemenst zijn en steeds minder aansluiten op hun risicomanagement- en complianceverplichtingen.

Het SaaS-model lost dit probleem op. Door de verantwoordelijkheid voor de infrastructuur over te dragen aan een gespecialiseerde leverancier zijn enterprisefuncties beschikbaar tegen voorspelbare kosten, worden compliance-eisen ondersteund en is eigen infrastructuurinspanning niet langer nodig.

De PIAM Suite van ID-ware als SaaS is de logische volgende stap in fysiek toegangsmanagement. Met Europese hosting en een eigen Platform Engineering Team biedt ID-ware een sterke basis waarop organisaties kunnen bouwen.

ID-ware is een toonaangevende wereldwijde leverancier van oplossingen voor fysiek identiteits- en toegangsbeheer (**PIAM = Physical Identity and Access Management**). Met meer dan 20 jaar ervaring hebben we ons gespecialiseerd in de implementatie van effectieve identificatie- en authenticatieprocessen om met name grote organisaties te ondersteunen. Door onze innovatieve en veilige producten in combinatie met het principe van langdurige partnerschappen bieden we onze klanten oplossingen op maat.