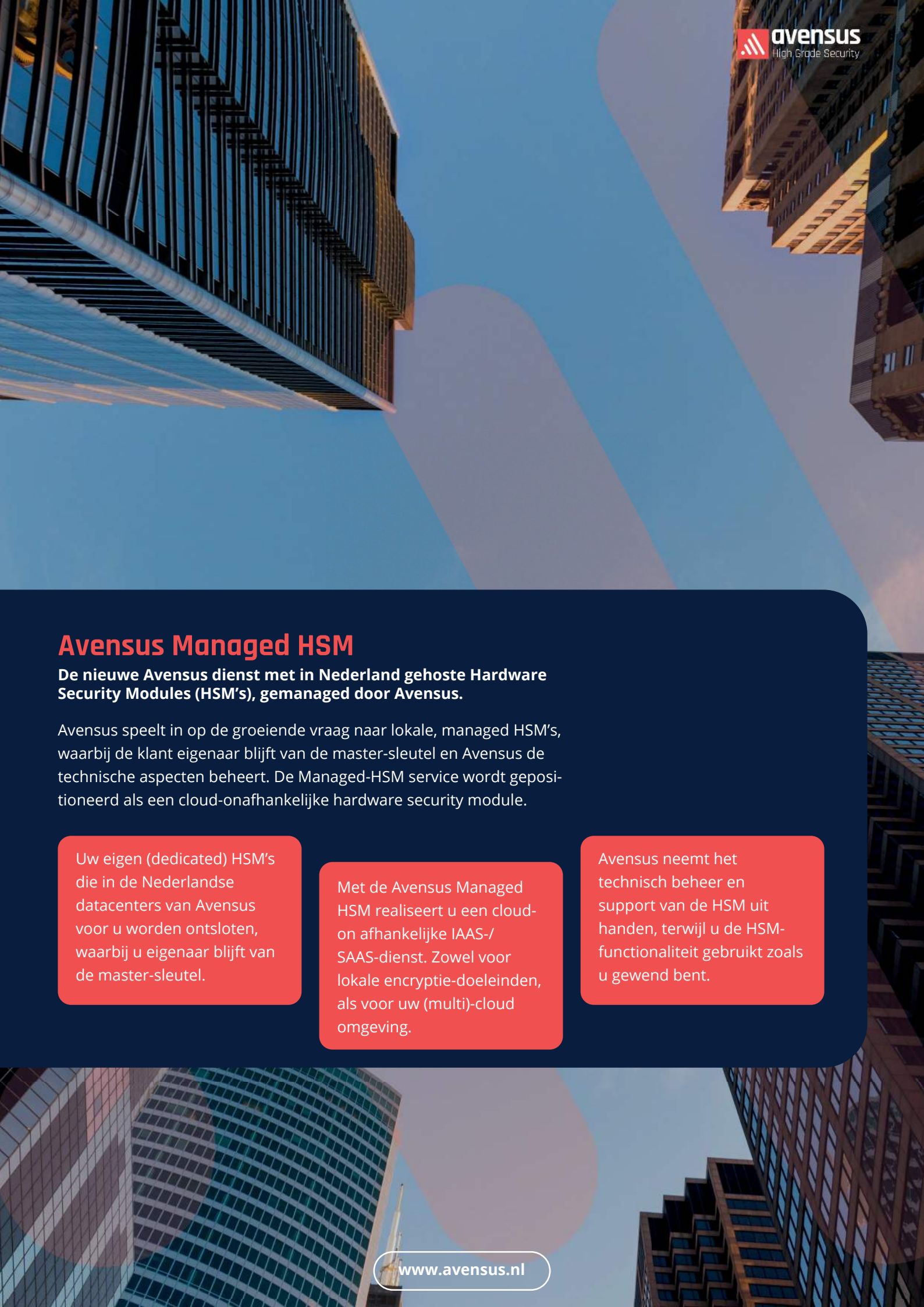


avensus
High Grade Security

Avensus Managed HSM

De nieuwe Avensus dienst met in Nederland gehoste Hardware Security Modules (HSM's), gemanaged door Avensus.

Avensus speelt in op de groeiende vraag naar lokale, managed HSM's, waarbij de klant eigenaar blijft van de master-sleutel en Avensus de technische aspecten beheert. De Managed-HSM service wordt gepositioneerd als een cloud-onafhankelijke hardware security module.

Uw eigen (dedicated) HSM's die in de Nederlandse datacenters van Avensus voor u worden ontsloten, waarbij u eigenaar blijft van de master-sleutel.

Met de Avensus Managed HSM realiseert u een cloud- on afhankelijke IAAS-/ SAAS-dienst. Zowel voor lokale encryptie-doeleinden, als voor uw (multi)-cloud omgeving.

Avensus neemt het technisch beheer en support van de HSM uit handen, terwijl u de HSM-functionaliteit gebruikt zoals u gewend bent.

www.avensus.nl

Avensus Managed HSM

Waaruit bestaat de Avensus Managed HSM?

De HSM bestaat uit de volgende onderdelen:

- standaard dubbel uitgevoerde HSM's, geplaatst in 2 verschillende datacenters, 24*7 service, ongeacht uw HSM inzet ('Acceptatie' of 'Productie').

1.
Volledig overzicht van de HSM-functionaliteit en activiteiten (zoals u dit vandaag zelf uitvoert), waarbij Avensus het Support verleent op de HSM's.

2.
Toegang tot de Avensus Managed HSM vanaf uw locatie en werkplek (via Smartcards).

3.
Met uw Managed HSM kunt u toegang realiseren tot uw Cloud-data.

4.
Met uw Managed HSM kunt u toegang realiseren tot uw on-premise data.

5.
Avensus voert technisch beheer & support uit van uw HSM-omgeving.

6.
De certificeringen van de Avensus DC's: ISO-14001, ISO-9001, ISO-2701, ISAE3402, PCI-DSS & NEN7510.

Een aantal business-specifieke kenmerken van deze service

Geen kapitaalbeslag
Avensus is eigenaar van de HSM's die voor de dienstverlening worden gebruikt. U hoeft niet zelf te investeren in de benodigde HSM-technologie.

Heldere Prijsstelling
De prijs van de dienstverlening omvat de datacenter hosting van de HSM's en het technische beheer & support. Hiervoor worden dus geen separate kosten in rekening gebracht.

Snel aan de slag met hardware-cryptografie
U hoeft geen in-house technische HSM-kennis op te bouwen, anders dan kennis over de te gebruiken functionaliteit voor uw HSM's.

Voorspelbare TCO
Omdat u het geheel van uw behoeften op HSM-gebied als dienst van Avensus afneemt, is de total cost of ownership transparant en voorspelbaar.

Regie op compliance
U houdt zelf de regie op uw compliance-behoeften. Uw auditoren (certifi cering ISO, GDPR, ETSI, SOC2, DORA of NIS2 e.d.) verkrijgen inzicht in de inrichting van de systemen en bedrijfsprocessen die in de Avensus dienstverlening worden gebruikt.

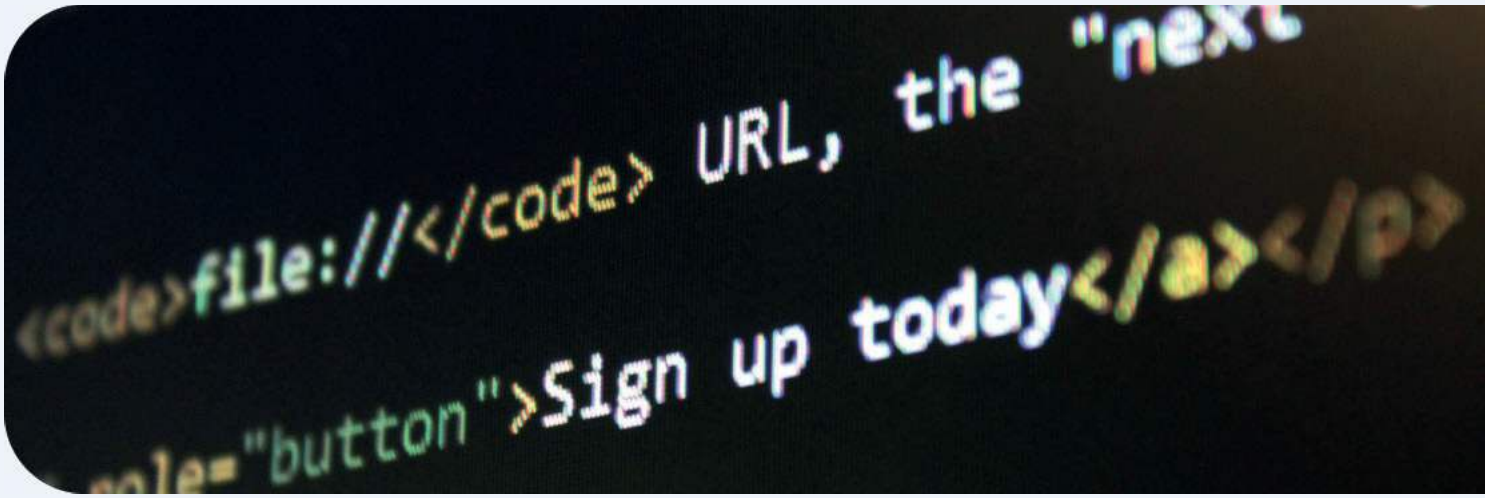
State of the art HSM's
Avensus zet voor haar Managed HSM Service uitsluitend de beste HSM's in van gerenommeerde vendoren.

Controle over uw door de HSM versleutelde applicatie-data
U verlaagt uw businessrisico richting de cloud: u heeft als enige toegang tot uw bedrijfskritische data, doordat u effectief de beschikking heeft over uw masterkey. Dat betekent dat uw CSP niet bij deze data kan, omdat u zelf de masterkey-eigenaar bent.

Geen Cloud Service Provider lock-in
Deze service is voor elke cloud-omgeving in te zetten, waardoor er geen lock-in situatie ontstaat bij één cloud service provider (CSP). Dit betekent dat uw data gemakkelijk kan worden ingezet bij een alternatieve CSP.

Digitaal soeverein
U speelt in op de huidige ontwikkelingen op het gebied van shared responsibility (uw organisatie is 'digitaal soeverein'), doordat Avensus de verantwoording neemt voor housing en technisch beheer & support van de HSM's en u eigenaar blijft van de masterkey.

Nederlandse jurisdictie
De Avensus Managed HSM valt uitsluitend onder de rechtsmacht van Nederland. Aangezien u zelf uw sleutels beheert, kunnen buitenlandse overheden niet zonder uw medewerking–of zonder medewerking van de Nederlandse rechter–uw sleutels gebruiken om uw data te ontsluiten.



HSM's zijn een 'Root of Trust' voor diverse toepassingen

- HSM-technologie is onontbeerlijk voor de bescherming van de Public Key Infrastructure (PKI) en PKI-Overheid. Avensus Managed HSM kan goed worden gecombineerd met PKI-as-a-Service of een on-premises PKI-oplossing.

- Overige toepassingen zijn zowel Internet of Things devices alsmede Identity of Things gerelateerde diensten als Privileged Access Management, TLS, private keys, digitale handtekeningen, eIDAS, E-documents, E-tickets, Code Signing en Time Stamping.

- Voor Centraal Sleutel Management vormt een HSM een gecertificeerde standaard om zo'n omgeving op een veilige manier te kunnen ontsluiten. Ook voor omgevingen waarin Cloud en Containers gebruikt worden.

- Certificaat Lifecycle Management vormt een nieuwe trend door de aangekondigde verlaagde levensduur van een digitaal certificaat van 12 maanden naar 90 dagen. Automatisering van het certificaatbeheer met een HSM als onderlegger is hierin cruciaal.

- Post Quantum Crypto (PQC) lijkt nog ver weg. Vertrouwt u erop dat uw huidige algoritmes en sleutelgroottes voorlopig nog voldoen? Zijn uw digitale sleutels al PQC-ready? En die in uw cloud ook? Post Quantum Readiness is testbaar. U kunt de Avensus Managed HSM dienst gebruiken als PQC test-HSM of als test voor andere typen algoritmes en sleutels.

Uw digitale sleutels betrouwbaar ondergebracht bij Avensus Nederland B.V.

Waarom zou u voor Avensus kiezen voor uw Managed HSM?

U beschermt uw lokale- en cloud-data door middel van een lokale, eigen digitale sleutel.

Uw Avensus Managed HSM's vallen onder Nederlandse wetgeving en -rechtsmacht (in lijn met GDPR, NIS2, DORA, etc.).

Avensus managed en host uw HSM's in gecertificeerde datacenters in Nederland.

Indien van toepassing: toegang tot datacenter is mogelijk (bijv. ter facilitering bij audits).

U hoeft zelf geen eigen technische encryptie-kennis (meer) te hebben.

Avensus heeft 35 jaar ervaring met encryptie-technologie met de benodigde certificeringen.

Technische specificaties

Waaruit bestaat de Avensus Managed HSM?

HSM Continuïteitsdienst

- Avensus host de HSM's in NL gecertificeerde datacenters en biedt 99.9% beschikbaarheid.
- De Avensus Managed HSM is inclusief 3 server connecties per HSM.
- Een HSM IAAS-/SAAS-dienst met de veiligheid en compliance van een on-premise HSM.
- Connectiviteit is gebaseerd op een VPN-verbinding.

Compliant via de HSM als Root of Trust

- Klant is en blijft eigenaar van de HSM master-sleutel.
- Door de klant gegenereerde HSM-sleutels kunnen beschermd worden door vertrouwde fysieke smartcards of sleuteldragers.
- HSM's en hostingomgeving voldoen aan alle relevante certificeringen zoals FIPS NIST 140-2 of 140-3 Level 2 of 3, eIDAS-High/Qualified en Common Criteria.
- De HSM is geschikt voor toegang tot uw cloud-data bij uw CSP's via uw eigen sleutel door gebruik van Bring-/Hold- Your Own Key (BYOK, HYOK) of Bring Your Own Encryption (BYOE).

Avensus houdt uw HSM technisch actueel

- De HSM blijft op een actueel niveau qua versiebeheer.
- Avensus heeft de hoogste technische-partner status bij HSM-fabrikanten.
- De dienstverlening is schaalbaar tot grote aantallen van gelijktijdige transacties (productie op industriële schaal).

Technische HSM kenmerken

- API-Support: PKCS#11, CAPI/CNG (Microsoft), OpenSSL, JAVA (JCE) en Web Services API.
- Ondersteunt de gebruikelijke asymmetrische algoritmes (RSA, Diffie-Hellman) en symmetrische algoritmes (AES, AES-GCM) en hash/message digest (SHA-1, SHA-2: 224, 256, 384, 512 bit).
- Full Suite B implementatie met licentie voor ECC, inclusief Brainpool en 'custom curves'.

Opties

Er zijn diverse opties mogelijk, mits ondersteund. Voor Test-doeleinden een enkelvoudig uitgevoerde HSM met 8*5 dekkende service. Bijvoorbeeld: licentie voor alternatieve algoritmes, Cloud Key Management, Enterprise/Central Key Management, Containers, Time Stamping services, technische Audit ondersteuning e.d.

Aanvullende diensten die mogelijk zijn (opties functioneel beheer)

- 'Security Officer'-rol als vertrouwelijke rol in uw Security- of Encryptie-organisatie.
- Participatie in Key-Ceremonie activiteiten, ofwel Quorum-deelname.
- Functioneel Beheer (voor als u zelf ook geen functionele HSM-kennis heeft).
- Uitbreiding van toepassingen of use-cases (zie 'Root of Trust' voor diverse toepassingen).

Over Avensus Nederland B.V.

Avensus Nederland B.V. is al meer dan 35 jaar partner van organisaties waarvoor encryptie-technologie van het hoogste bedrijfsbelang is. Een groot deel van de Nederlandse banken en verzekeraars, overheidsorganisaties en organisaties die deel uitmaken van de 'vitale infrastructuur' in Nederland en België vertrouwen op de kennis en ervaring van Avensus bij de installatie, onderhoud en service van hun HSM's.

Het motto van Avensus

Het motto van Avensus is 'Encrypt all and manage the keys yourself'. Voor veel compliance-driven organisaties is dit een must. Bij de overgang naar een 'cloud-tenzij-architectuur' blijkt dit motto meer dan ooit valide. Als uw IT ook aan het verschuiven is naar de cloud, is ook uw encryptie-strategie onderhevig aan een transformatie.

U wilt uw (bedrijfskritische) gegevens ook in uw cloud-omgeving veilig ontsluiten. Om zeker te weten dat uw data ook in een cloud-omgeving veilig is, dient u zelf uw eigen encryptie (master-)sleutels te blijven gebruiken en managen. Juist om te voldoen aan compliance eisen én het securitybeleid van uw organisatie.

Avensus Nederland B.V. is onderdeel van de Confido Groep, een Nederlandse holding van bedrijven die zich toeleggen op digitale vertrouwensdiensten. Zie voor meer informatie www.confido.eu/nl.

Het motto van Avensus is
'Encrypt all and manage the keys yourself'.

Neem contact op

Benader Avensus voor het maken van een afspraak of het inwinnen van meer informatie over de Avensus Managed HSM dienst. Dit kan via een e-mail aan: sales@avensus.nl.

U kunt ook de Senior Sales Manager bellen die alles weet van deze dienst. Hij informeert u graag: Martin Szendy, 06-21214020.