Technolution
Prime

Netwerk-encryptie oplossingen

Veilige verbindingen tussen gerubriceerde netwerken

Redefining **solutions**

“De netwerken van de overheid liggen voortdurend onder vuur van aanvallen door statelijke actoren. **Hoogwaardige encryptie is onmisbaar voor onze nationale veiligheid.** Onze encryptie-oplossingen beschermen de gevoelige informatie van overheid en burgers tegen aanvallers.”

Jonathan Hofman
Business Unit Director High Assurance

Technolution
Prime

Inhoud

Veilige verbindingen in een onveilige wereld

Het belang van betrouwbare encryptie is groter dan ooit voor overheidsorganisaties. De geopolitieke situatie in de wereld is voorgoed veranderd. In cyberspace woedt een onzichtbare oorlog waarin cyberaanvallen en digitale spionage dagelijkse realiteit zijn.

De ICT-infrastructuur van ministeries, agentschappen en andere overheidsorganisaties ligt continu onder vuur van aanvallers. Vaak zijn dit ‘statelijke actoren’: professionele individuen en organisaties die door hun land gesteund worden en beschikken over vrijwel onbeperkte middelen. In deze digitale wapenwedloop beschermt encryptie de vertrouwelijkheid en integriteit van gevoelige informatie.

Het strategisch belang van encryptie
Hoogwaardige encryptie is een onmisbaar onderdeel van onze nationale veiligheid. Zonder robuuste versleuteling lopen ministeries het risico dat buitenlandse mogendheden kritieke informatie onderscheppen of manipuleren. Encryptie beschermt internationale samenwerking, diplomatieke communicatie en defensie-inlichtingen. Ook nationaal is encryptie belangrijk. Het ondersteunt het vertrouwen tussen overheid en burgers. Burgers verwachten dat hun gegevens veilig worden beheerd, en overheidsorganisaties hebben veilige digitale infrastructuren nodig om hun beleid uit te voeren.

Veilige verbindingen, ook voor de toekomst
Veel cyberaanvallen zijn gericht op het achterhalen van geheime informatie via de externe dataverbindingen van beveiligde netwerken. Vooral verbindingen tussen verschillende locaties via een open, onvertrouwd netwerk zoals het internet zijn gevoelig voor aanvallen. Een aanvaller die toegang krijgt tot een dataverbinding heeft een ingang in de verbonden netwerken en kan data onderscheppen en ontcijferen.

Met PrimeLink netwerkvercijferaars wordt data versleuteld vóór verzending over een dataverbinding en na ontvangst ontsleuteld. Zonder de bijbehorende encryptiesleutels is de data onleesbaar. Hierbij is de methode van encryptie van belang om maximale weerbaarheid tegen aanvallen te garanderen. Met de komst van kwantumcomputers is encryptie in de toekomst, ook met grotere sleutels, namelijk niet meer altijd veilig. Daarom gebruiken PrimeLinks encryptiemethodes die ‘kwantumresistent’ zijn; deze encryptie kan zelfs niet worden gekraakt door een kwantumcomputer.

Kwantumresistentie en post-kwantum cryptografie

Kwantumcomputers zijn nog niet praktisch toepasbaar voor encryptie. Toch speelt kwantumtechnologie een grote rol in encryptie, omdat een kwantumcomputer theoretisch vele malen sneller is dan binaire computers. Zodra er een kwantumcomputer met voldoende ‘qubits’ wordt ontwikkeld, worden heel veel cryptografische algoritmes kwetsbaar voor het kraken van de versleuteling. Naar verwachting zal dit ergens tussen 2030 en 2050 het geval zijn.

Er zijn gelukkig encryptiemethodes die niet bezwijken onder de kracht van de kwantumcomputer, zoals 256 bits, symmetrische, kwantumresistente sleutels en post-kwantum cryptografie. Dankzij deze methodes zijn onze PrimeLinks vandaag al voorbereid op aanvallen door kwantumcomputers in de toekomst.

Geëvalueerde encryptie voor gerubriceerde informatie
De Unit Weerbaarheid van de AIVD biedt Nederlandse overheidsinstellingen een overzicht van geëvalueerde oplossingen voor de bescherming van gerubriceerde informatie. Bij elk geëvalueerd product geeft de Unit Weerbaarheid een inzetadvies. Het inzetadvies bevat voorwaarden en richtlijnen voor inzet van de producten voor het betreffende rubriceringsniveau, van Departementaal VERTROUWELIJK, tot en met Staatsgeheim ZEER GEHEIM.

FPGA's – de veiligheid van hardware, de flexibiliteit van software

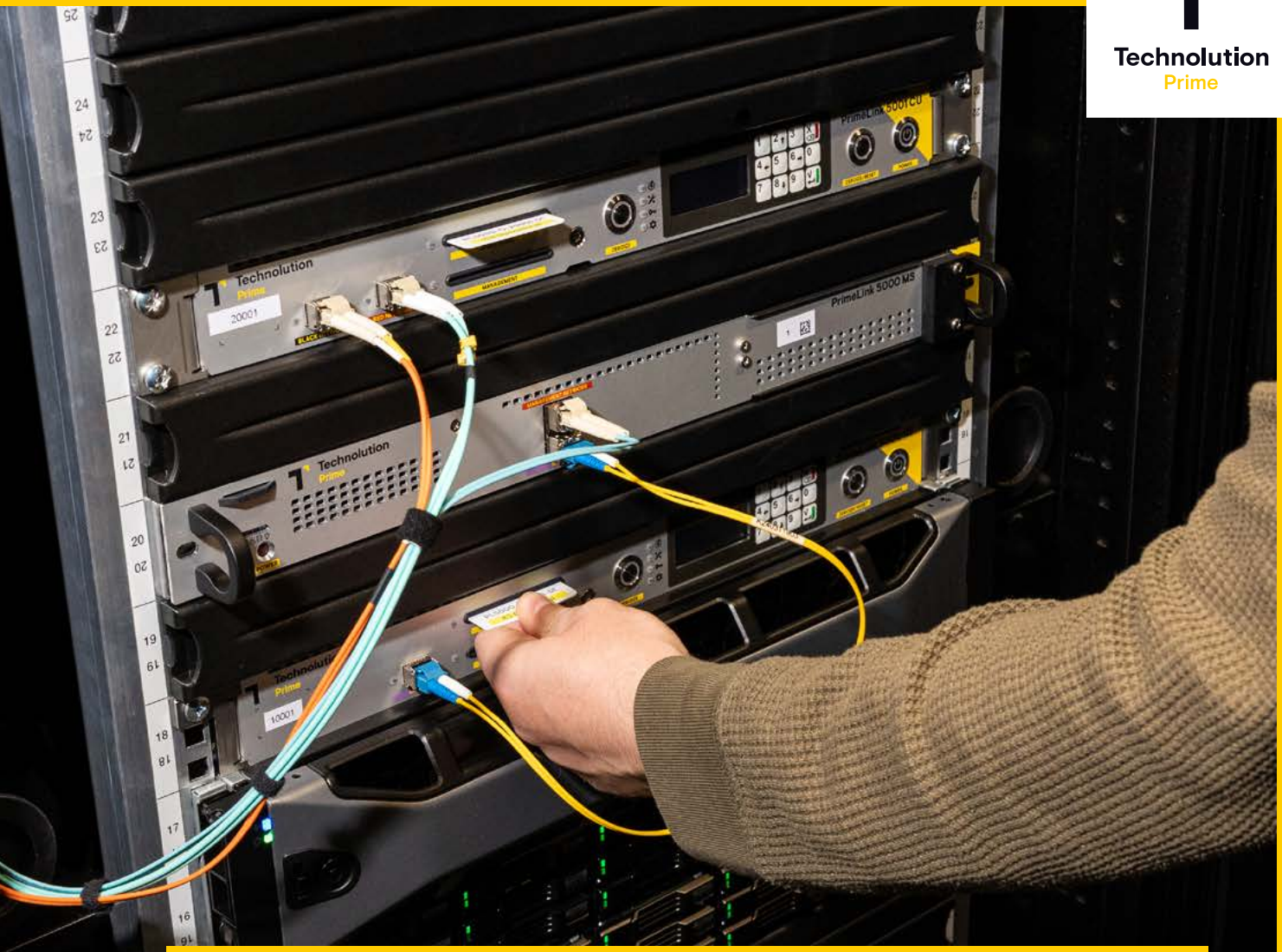
Onze beveiligingsproducten worden intern aangedreven door Field-Programmable Gate Arrays oftewel FPGA's. Deze programmeerbare chips worden voorzien van firmware in een speciale taal. Ze voeren cryptografische algoritmen parallel uit. Daardoor zijn ze razendsnel, efficiënt en is er een minimaal risico op interferentie tussen processen. Omdat cryptografische sleutels en bewerkingen in gescheiden logische blokken worden uitgevoerd, zijn FPGA's zeer veilig. De sleutels zijn strikt afgeschermd voor andere componenten in of buiten de FPGA.

Het grote voordeel van FPGA's is dat ze herprogrammeerbaar zijn, bijvoorbeeld met nieuwe cryptografische standaarden, beveiligingsupdates of functionaliteiten. Daardoor kan de functionaliteit van de PrimeLinks steeds weer worden vernieuwd en aangepast. Updates kunnen nieuwe features bevatten, zoals een doorvoersnelheid van 10 Gbit/s in plaats van 1 Gbit/s, of de introductie van een nieuw cryptografisch algoritme. Zo groeit de netwerkvercijfering mee met de behoeftes van de gebruiker en de laatste eisen op het gebied van veiligheid. De hardware hoeft daarvoor niet te worden vervangen. FPGA's slaan zo een brug tussen hardwarematige betrouwbaarheid en softwarematige wendbaarheid.

De PrimeLink encryptieoplossingen van Technolution Prime zijn stuk voor stuk geëvalueerd door de Unit Weerbaarheid. Daar zijn ook de inzetadviezen op te vragen.

De werkwijze van Technolution Prime
Technolution is op het gebied van geëvalueerde encryptie en domeinscheiding marktleider in Nederland. Onder de merknaam Technolution Prime ontwikkelen en produceren wij netwerkvercijferaars, datadiodes, datafilters en andere High Assurance veiligheidsproducten. Daarbij is 'Separation of Concerns' het leidende uitgangspunt. Daarnaast ontwikkelen wij maatwerkoplossingen op projectbasis en bieden wij ondersteuning, cryptobeheer en advies bij beveiligingsvragen, met name voor overheidsorganisaties.

Voor maximale flexibiliteit en veiligheid maken wij gebruik van FPGA's, oftewel (her)programmeerbare chips. Hierdoor zijn de Prime-producten niet alleen snel, maar ook flexibel en toekomstvast – ze worden regelmatig bijgewerkt met nieuwe functionaliteiten of eigenschappen.



Separation of Concerns

Bij al onze High Assurance oplossingen is het uitgangspunt: 'Separation of Concerns'. Dit ontwerpprincipe is essentieel voor de beveiligingswaarde van onze oplossingen. Het schrijft voor dat elke component een duidelijke, afgebakende taak heeft en uitsluitend die taak uitvoert. Functies die daar niet rechtstreeks bij horen, worden bewust buiten die laag gehouden. Dankzij deze scheiding is de betrouwbaarheid niet afhankelijk van complexe netwerkconfiguraties: een wijziging of verstoring in één laag heeft geen directe gevolgen voor de andere lagen.

Dat principe passen we consequent toe in onze ontwerpen, zowel in uw netwerkarchitectuur als in de interne functionaliteit van PrimeLinks. Het resultaat zijn oplossingen die inherent veilig zijn dankzij helderheid en eenvoud.

Architectuur In een netwerkarchitectuur heeft iedere laag zijn eigen rol, bijvoorbeeld routing, switching of transport. De encryptie vormt een zelfstandige, transparante laag die zich richt op één taak: het beveiligen van de communicatie, ongeacht de netwerkconfiguratie of -topologie. De cryptografische functies van de PrimeLinks zijn daarmee strikt gescheiden van de omliggende netwerkapparatuur. Daardoor blijft de beveiliging intact, ongeacht hoe het netwerk is opgebouwd of beheerd.

Functionaliteit Ook binnen de PrimeLinks zelf is de scheiding in lagen zichtbaar. Allereerst is er de laag met het beveiligde domein, de 'rode' kant. Vervolgens de encryptielaag, die de data versleutelt en beschermt. Daarboven de managementlaag voor monitoring en beheer. Tot slot de publieke laag, de 'zwarte' kant: het gedeelde netwerktransport dat de versleutelde data veilig doorstuurt. Iedere laag heeft zijn eigen taak; functies en verantwoordelijkheden worden niet gedeeld. Dit verhoogt de voorspelbaarheid en vormt de basis voor het hoge beveiligingsniveau van PrimeLinks.

PrimeLink

Hoogwaardige encryptie van Nederlandse bodem

De PrimeLink encryptieproducten worden gekenmerkt door eenduidige, doelmatige functionaliteit, gekoppeld aan snelheid en flexibiliteit. Dit is het resultaat van onze ontwerpfilosofie van ‘Separation of Concerns’ en van het gebruik van FPGA’s: programmeerbare chips. Deze krachtige combinatie vormt de kern van filosofie van Technolution Prime: heldere architectuur, maximale veiligheid en aanpasbare functionaliteit.

Gegarandeerde betrouwbaarheid
De betrouwbaarheid van onze beveiligings-oplossingen voor overheidsorganisaties moet onomstotelijk vaststaan. Een zeer grondig test-traject, gecombineerd met uiterst complete documentatie en de evaluatie door de Unit Weerbaarheid van de AIVD zijn belangrijke stappen om dit te bewijzen.

Supplychain
Elektronicacomponenten komen doorgaans uit verschillende landen – en dat zijn niet altijd bevriende landen. Daarom hebben wij onze belangrijkste leveranciers van componenten in de supplychain kritisch geselecteerd. Bovendien leggen wij hen aanvullende controles en eisen op. Zo hebt u de zekerheid dat uw encryptie-apparatuur is gerealiseerd met veilige componenten.

Assemblage
Vanuit het oogpunt van betrouwbaarheid voeren wij de assemblage van onze producten volledig in eigen huis uit. Hierbij gelden dezelfde strenge normen als bij de ontwikkeling. Het werk wordt uitgevoerd door gescreende medewerkers, op een afzonderlijke, beveiligde locatie die voldoet aan de hoge eisen van de Nederlandse overheid. Zo borgen we niet alleen de technische kwaliteit, maar ook de vertrouwelijkheid en integriteit van elk product.

Technolution
Prime

De encryptieproducten van Technolution Prime

PrimeLinks bieden hoogwaardige, gerubriceerde encryptie van Nederlandse bodem.

PRIMELINK 3015+

Netwerkvercijferaar voor rubriceringsniveau **Departementaal VERTROUWELIJK** en **Stg. CONFIDENTIEEL**

- 1 én 10 Gbit/s, laag 2 én 3, kwantumresistent, Non-CCI
- Online monitoring en remote beheer
- Mogelijkheid voor versleutelde verbinding met OpenVPN softwareclients
- Geschikt voor Stg. CONFIDENTIEEL vanaf firmware v2.0.0.0 in situaties zonder APT's (Advanced Persistent Threats)

PRIMELINK 4010

Lijnvercijferaar voor rubriceringsniveau **Stg. (ZEER) GEHEIM**

- 10 Gbit/s, hoge snelheid, maximale bandbreedte op laag 2
- Minimale beheerlast
- Kwantumresistent

PRIMELINK 5001

Onder evaluatie

IP-vercijferaar voor **Stg. (ZEER) GEHEIM**

- 1 Gbit/s, laag 3, kwantumresistent
- Gebruiksvriendelijk beheer, ontwikkeld in nauwe samenwerking met eindgebruikers
- Geoptimaliseerd voorraadbeheer en sleutelplan voor snellere implementatie, slimmere logistiek
- Ook beschikbaar als PrimeLink 5001c voor Stg. CONFIDENTIEEL

Ecosystemen voor encryptie

De PrimeLink netwerkvercijferaars doen hun werk in uw organisatie discreet, ondersteund door doordachte eco-systemen voor beheer en monitoring. Deze systemen geven uw netwerkbeheerders stevige grip op hun netwerk-configuraties. Bovendien leveren de systemen heldere inzichten in de prestaties van de versleutelde verbindingen.

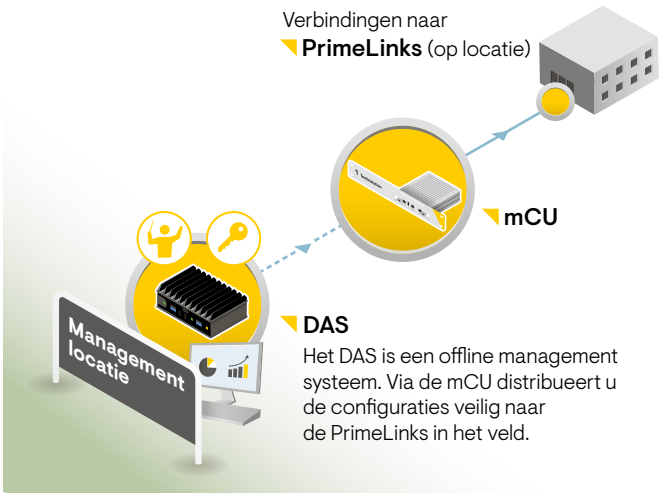
PrimeLink 3015+
Centraal beheer met het DAS

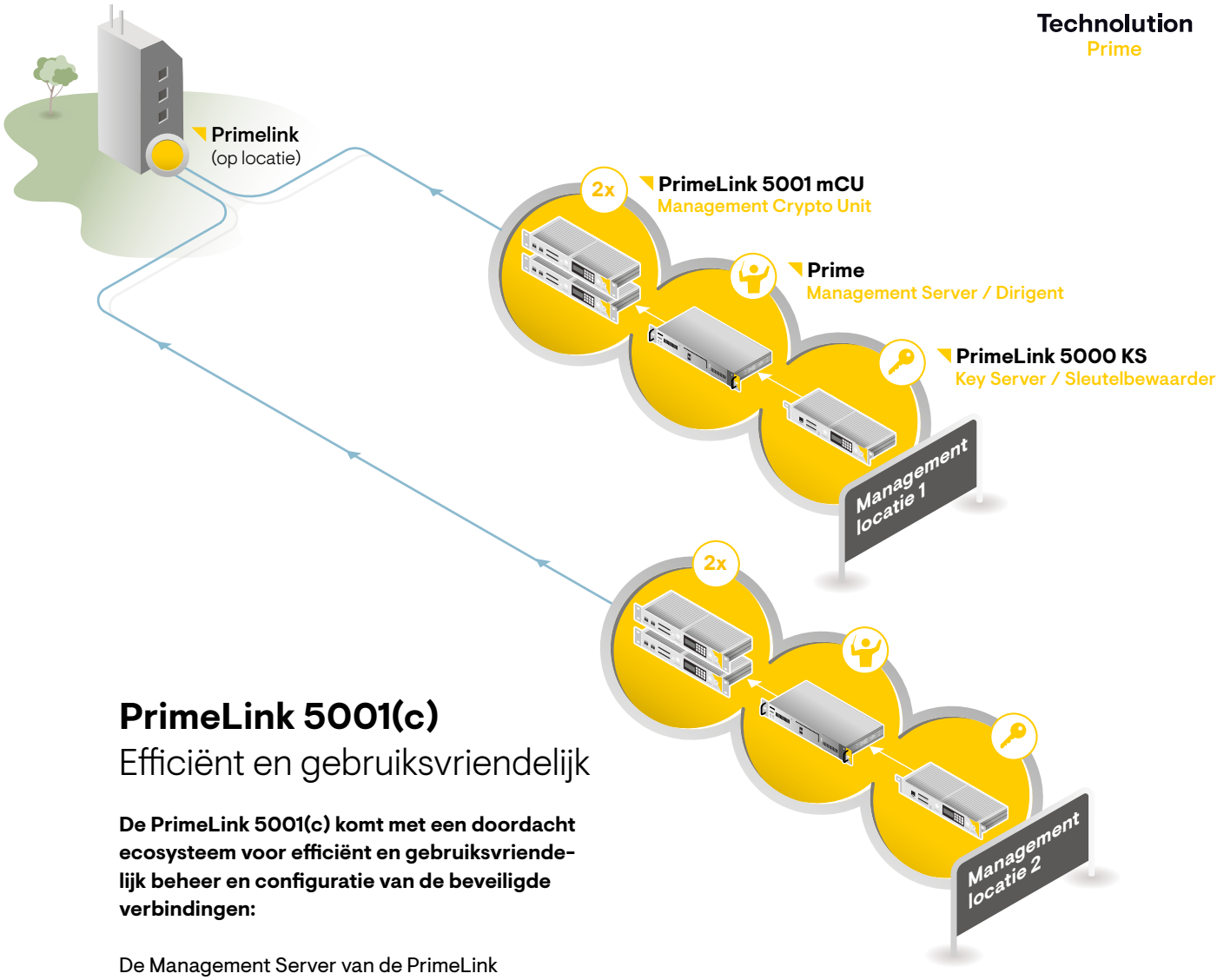
Het hart van het beheer voor de PrimeLink 3015+ wordt gevormd door het Domain Administration Station.

Het Domain Administration Station (DAS) is een speciaal systeem dat een unieke configuratie-image genereert voor iedere PrimeLink 3015+ in een netwerkdomein. Beheerders distribueren deze images online via de Management Crypto Unit of offline via USB-sticks. Met een overzichtelijk systeem van netwerkdomeinen en groepen van PrimeLinks kan de netwerkbeheerder een brede selectie aan beveiligde netwerkconfiguraties maken, beheren en monitoren.

- **Online** monitoring en beheer
- **Remote** updates
- **Hitless updates** – het netwerk blijft actief (beschikbaar vanaf firmware v3.0.0.0)
- **Één of meer managementlocaties** waarvandaan het netwerk wordt beheerd

Het ecosysteem van de PrimeLink 3015+	
Crypto Unit (CU)	De “verbinder”. De PrimeLink 3015+ Crypto Units die de beveiligde verbindingen opbouwen voor het dataverkeer.
Domain Administration Station (DAS)	De “dirigent” en “sleutel-bewaarder”. Een offline systeem dat de primaire interface is voor beheer en monitoring. Het DAS genereert en bewaart alle sleutels, certificaten en configuraties voor het opzetten van beveiligde verbindingen tussen CU’s.
Management Crypto Unit (mCU)	Een CU die optreedt als een beveiligde managementverbinding tussen het DAS en de CU’s in het netwerk.





PrimeLink 5001(c)

Efficiënt en gebruiksvriendelijk

De PrimeLink 5001(c) komt met een doordacht ecosysteem voor efficiënt en gebruiksvriendelijk beheer en configuratie van de beveiligde verbindingen:

De Management Server van de PrimeLink 5000-serie biedt een gebruiksvriendelijke grafische interface voor het creëren en beheren van netwerkconfiguraties. Beheerders creëren met een paar klikken een beveiligd netwerk. Netwerkconfiguraties en IP-routingtabellen worden vervolgens automatisch gegenereerd. Via de Management Crypto Unit kan de nieuwe netwerkconfiguratie eenvoudig worden gedistribueerd naar alle PrimeLinks in het netwerk.

- Eenvoudig **online beheer en configuratie** dankzij unieke gebruikersinterface
- Eenvoudig **gecentraliseerd voorraadbeheer**
- Eenmalig contact met **Nationale Distributie Autoriteit** voldoet
- Na installatie kunt u uw netwerk **permanent zelf beheren** en in stand houden dankzij geoptimaliseerd sleutelplan

Het ecosysteem van de PrimeLink 5001(c)	
Crypto Unit (CU)	De “verbinder”. De PrimeLink 5001(c) Crypto Units die de beveiligde verbindingen opbouwen voor het dataverkeer.
Management Server (MS)	De “dirigent”. Voert het beheer en de configuratie van de CU’s in het veld uit en is de primaire interface voor het beheer.
Key Server	De “sleutelbewaarder”. Genereert de sleutels die via de MS en de Management CU worden gedistribueerd naar de CU’s met de beveiligde verbindingen.
Management Crypto Unit (mCU)	Een CU die optreedt als een beveiligde management-verbinding tussen de MS en de CU’s in het netwerk.

Encryptie van verbindingen

Netwerk-encryptie **in de praktijk**

Welke encryptieoplossing past bij uw organisatie?

Dit hangt af van verschillende factoren. Sommige daarvan zijn inhoudelijk, zoals de activiteiten van uw organisatie, de gevoeligheid van de informatie en de rubricering. Andere factoren zijn technisch, zoals het type netwerk, het aantal beveiligde verbindingen en de benodigde bandbreedte. Ook organisatorische aspecten spelen een rol, zoals de omvang en de expertise van uw beheer-organisatie. Wij adviseren u graag over de beste opties voor uw specifieke situatie.

Op de volgende pagina's ziet u een aantal illustratieve voorbeelden.


Technolution
Prime

USE**CASE 1**

Veilige point-to-pointverbindingen met hoge bandbreedte

Interconnectiviteit datacenters

SITUATIE

Een data-intensieve overheidsorganisatie werkt met hooggerubriceerde informatie. De organisatie heeft twee primaire datacenters en een derde datacenter voor backup. Confidentialiteit en continuïteit zijn cruciaal. Alles wat in datacenter 1 wordt opgeslagen, wordt daarom realtime gesynchroniseerd met datacenter 2. Als datacenter 1 uitvalt, neemt datacenter 2 zonder tijdverlies alle taken over. Het back-updatacenter, datacenter 3, fungeert als digitaal vangnet. De data van de primaire datacenters wordt hier periodiek naar 'afgestort'. Bij grote calamiteiten, bijvoorbeeld uitval van beide primaire datacenters, wordt alle data van de organisatie vanuit het back-updatacenter hersteld.

DE UITDAGING

De organisatie genereert grote data-stromen. De realtime synchronisatie tussen de primaire datacenters en de offload naar de back-up gebeuren via dedicated point-to-pointverbindingen. De bandbreedte van de verbindingen moet groot genoeg zijn om al deze stromen met zeer gevoelige informatie te verwerken. Dit vraagt om snelle encryptie met lage latency die bovendien moet voldoen aan hoge rubriceringseisen.

DE OPLOSSING

De PrimeLink 4010 en de PrimeLink 3015+ (voor Dep-V) bieden beide voldoende bandbreedte voor de point-to-point-verbindingen tussen de datacenters.

PrimeLink 4010

Hoge snelheid, hoge rubricering, minimale beheerlast

De PrimeLink 4010 wordt altijd in tweevoud geleverd. Beide apparaten accepteren alleen data van elkaar. De PrimeLink 4010 functioneert op 10 Gbit/s en is speciaal ontworpen voor datacenters.

- Laag 2 **point-to-point-encryptie**
- Bandbreedte **10 Gbit/s**
- Tot en met **Stg. (ZEER) GEHEIM**

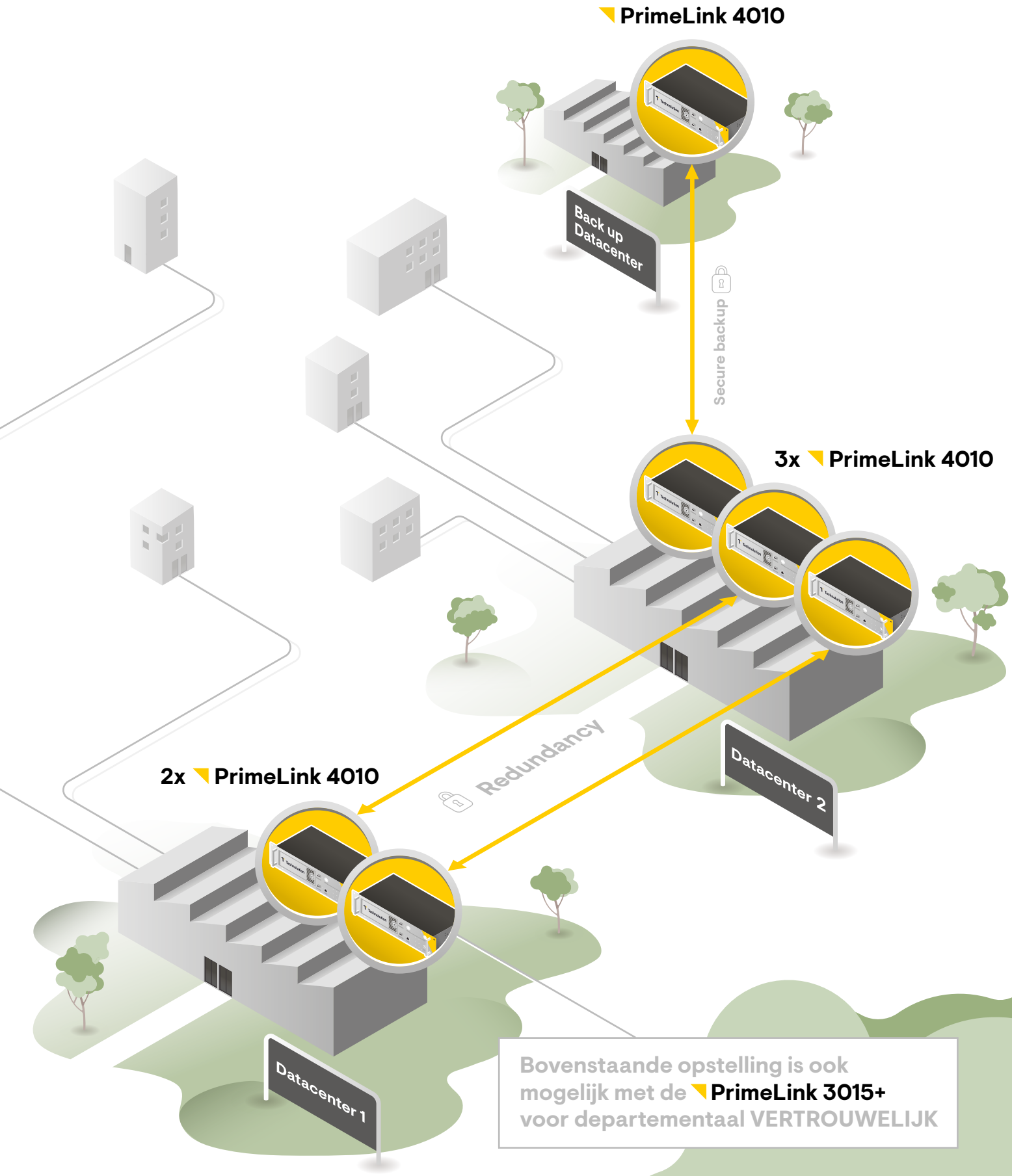
PrimeLink 3015+

Flexibiliteit in snelheid en netwerkopties

De PrimeLink 3015+ biedt 1G en 10G bandbreedtes, zowel in een configuratie met laag 2 point-to-point lijnvercijfering als in een configuratie met laag 3 IP-vercijfering. Deze netwerkvercijferaar is daardoor inzetbaar in vrijwel alle netwerkconfiguraties.

- Laag 2 **point-to-point-encryptie**
- Laag 3 **encryptie voor IP-netwerken**
- Bandbreedte **1 Gbit/s** of **10 Gbit/s**
- Tot en met **Departementaal VERTROUWELIJK** of **Stg. CONFIDENTIEEL***

* Vanaf firmware v2.0.0.0, in situaties zonder dreiging van statelijke actoren



Bovenstaande opstelling is ook mogelijk met de **PrimeLink 3015+** voor departementaal VERTROUWELIJK

USE**CASE 2**

Maximale flexibiliteit in netwerkconfiguraties

Encryptie tussen overheidslocaties

SITUATIE

De medewerkers van deze overheidsorganisatie werken op uiteenlopende locaties. De organisatie heeft vestigingen in het hele land die onderling data uitwisselen. De informatie van de organisatie is gerubriceerd als Departementaal VERTROUWELIJK. Continue beschikbaarheid van deze informatie is vereist.
De medewerkers werken met de gerubriceerde informatie en doen dit ook vanaf hun thuiswerkplek. Daarvoor hebben zij toegang nodig tot het netwerk. Hun werkdossiers worden realtime gesynchroniseerd en de medewerkers downloaden vaak grote bestanden. Ook videovergaderen en remote access-sessies vragen veel bandbreedte.

DE UITDAGING

Er zijn geen 'dedicated' verbindingen tussen vestigingen; alle verbindingen van het netwerk, waaronder de verbindingen met thuiswerkers, lopen over het internet. Er is geen behoefte aan een zeer grote bandbreedte, maar schaalbaarheid is wel vereist – zowel wat betreft bandbreedte, als wat betreft het aantal verbindingen. De gekozen oplossing moet geschikt zijn voor de rubricering Departementaal VERTROUWELIJK en op termijn een full mesh netwerk. De thuiswerkers hebben behoefte aan een oplossing die minimale impact heeft op hun thuiswerksituatie, maar wel een veilige verbinding biedt.

DE OPLOSSING

PrimeLink 3015+

Post-kwantum cryptografie voor Departementaal VERTROUWELIJK

De dataverbindingen tussen de vestigingen worden versleuteld met de PrimeLink 3015+. Deze is op OSI-laag 3 geconfigureerd als 'hub-and-spoke'. De configuratie is flexibel; een full mesh configuratie, waarbij het netwerk volledig is vermaasd, is bijvoorbeeld ook mogelijk. De PrimeLink 3015+ biedt kwantumresistentie, is geëvalueerd voor Departementaal VERTROUWELIJK en heeft een bandbreedte van naar keuze van 1 Gbit/s of 10 Gbit/s. Netwerkupdates worden geïmplementeerd zonder netwerkonderbrekingen.

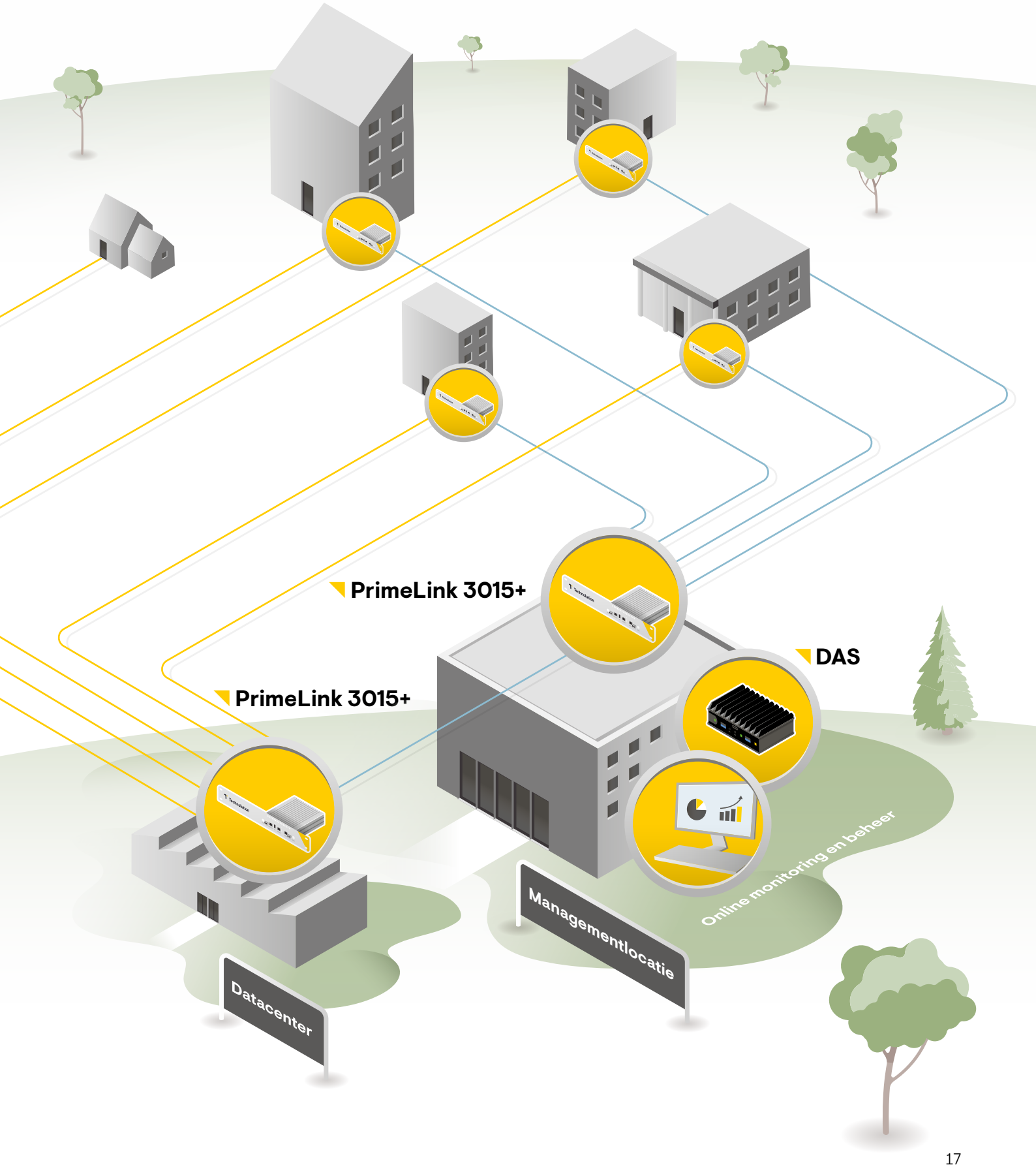
De thuiswerkende medewerkers krijgen een softwareclient op hun computer die direct verbinding maakt met een PrimeLink 3015+ in het organisatienetwerk. Deze softwareclient is compatibel met de PrimeLink 3015+ maar heeft een lagere encryptiesnelheid. N.B. Een softwareclient op een medewerker-pc is inherent minder veilig dan de hardware-encryptie van de PrimeLink 3015+. Aanvullende maatregelen zijn aan te bevelen.

DE OPLOSSING

Technolution
Prime

Versleutelde verbindingen

Managementtunnels



USECASE 3

Encryptie op grote schaal voor kritieke netwerken

Complexe, grootschalige, **hooggerubriceerde netwerken**

SITUATIE

Een grote overheidsorganisatie opereert op nationaal niveau. De organisatie heeft vestigingen en dependances op honderden locaties, die allemaal met elkaar zijn verbonden in een groot, gedeeltelijk vermaasd netwerk. De organisatie werkt met extreem gevoelige informatie tot en met rubricering Stg. ZEER GEHEIM. Een inbraak op de communicatielijnen van deze organisatie, bijvoorbeeld door een statelijke actor, zou tot grote problemen kunnen leiden.

DE UITDAGING

Ook al staat beveiliging op nummer één, voor deze organisatie is een robuuste oplossing met eenvoudig beheer een belangrijke eis. Hoge beschikbaarheid van het complete netwerk (24/7) is essentieel. Daarnaast moeten beheerders het netwerk naar wens snel kunnen aanpassen of uitbreiden. De oplossing moet geschikt zijn voor de hoogste rubriceringen en bestand tegen toekomstige aanvallen met kwantum-computers.

DE OPLOSSING

PrimeLink 5001

Robuust, flexibel, gebruiksvriendelijk

De locaties van de organisatie worden met elkaar verbonden via PrimeLink 5001 IP-vercijferaars. Dit zijn dedicated verbindingen; de lokale netwerken worden met de PrimeLink 5001 direct via het internet gekoppeld. De PrimeLink 5001's accepteren alleen data van andere PrimeLink 5001's die hiervoor zijn geconfigureerd. Beheerders kunnen de configuratie eenvoudig aanpassen in een intuïtieve, gebruiksvriendelijke beheerapplicatie, die zelfs grote netwerken overzichtelijk maakt.

Het voorraadbeheer en het sleutelplan van de PrimeLink 5001 zijn optimaal afgestemd op de eisen van grote organisaties met decentrale infra-structuren. Slechts één interactie met de Nationale Distributie Autoriteit is nodig voor de initiële 'enrollment' van de managementomgeving. Daarna kan uw organisatie het netwerk permanent zelf beheren en in stand houden.

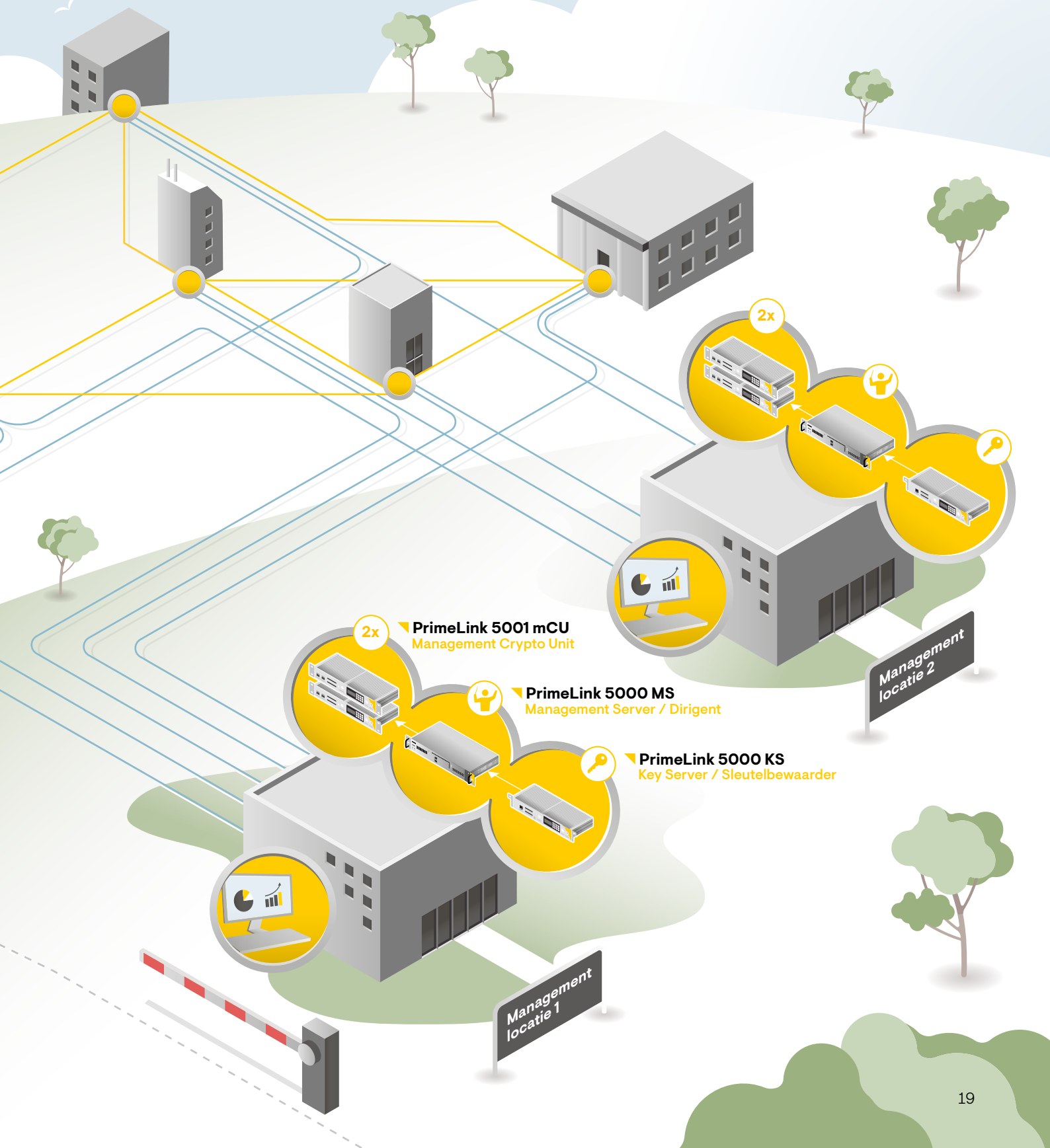
- Stg. **ZEER GEHEIM**
- **Full mesh** en andere configuraties
- **Post-kwantum** cryptografie
- **Dual Power Supply**, geschikt voor gebruik in datacenters
- **Centraal en decentraal** beheer
- Geoptimaliseerd **voorraadbeheer en sleutelplan**

DE OPLOSSING

Versleutelde verbindingen

Managementtunnels

Primelink (op locatie)



USE**CASE 4**

High Assurance encryptie op desktopformaat

Volwaardige encryptie voor elke locatie

SITUATIE

Een overheidsorganisatie onderhoudt dataverbindingen met buitenposten op afgelegen locaties. Snelle en betrouwbare uitwisseling van informatie is van levensbelang voor het personeel in de buitenposten, maar de verbindingen zijn instabiel en wisselen sterk in bandbreedte.

DE UITDAGING

Vanwege de beperkte ruimte zijn er op de buitenposten geen serverracks voor standaard 19'' encryptieapparatuur beschikbaar. De versleutelde verbinding met het hoofdkantoor heeft idealiter een hoge bandbreedte voor de snelle uitwisseling van grote hoeveelheden informatie. In de praktijk varieert dit echter sterk per buitenpost. De encryptie-eisen verschillen ook per buitenpost, maar zijn minimaal Departementaal VERTROUWELIJK en vaak hoger. Kwantumresistentie of post-kwantum encryptie is vereist, net als een hoge betrouwbaarheid van de beveiligde verbinding.

DE OPLOSSING

Desktopvarianten PrimeLink 3015+ en PrimeLink 5001

Compromisloze High Assurance encryptie

De desktopvariant van PrimeLink 3015+ en de PrimeLink 5001 leveren post-kwantum encryptie met de vereiste bandbreedte voor respectievelijk de rubriceringen departementaal VERTROUWELIJK en Stg. (ZEER) GEHEIM. Deze compacte varianten zijn speciaal ontworpen voor locaties waar de ruimte, de stroomvoorziening of de IT-infrastructuur beperkt zijn.

Ondanks de compacte vorm doen deze PrimeLinks geen concessies op het gebied van prestaties en specificaties; deze zijn vrijwel identiek aan de grotere 19''-versies. Zowel de PrimeLink 3015+ als de 5001 zijn geschikt voor beheer op afstand. Alle desktopvarianten kunnen functioneren in een netwerk waar verschillende bandbreedtes naast elkaar voorkomen.

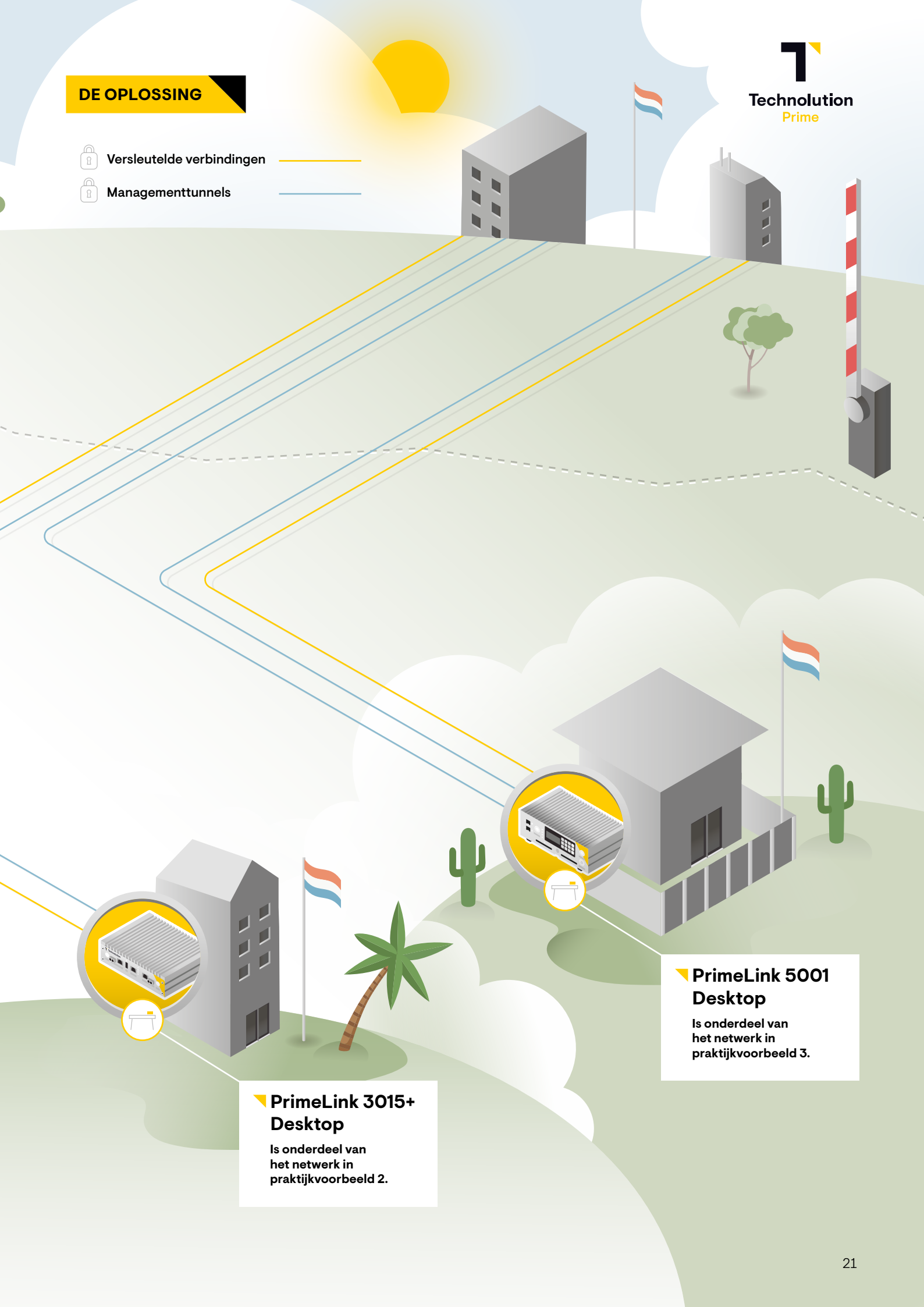
- **Desktopmodel** met compacte vormfactor
- Geschikt voor vrijwel **alle netwerkconfiguraties**
- Meerdere **bandbreedtes tegelijkertijd**
- **Geen concessies** ten aanzien van prestaties en beveiligings-kenmerken

DE OPLOSSING

Technolution
Prime

Versleutelde verbindingen

Managementtunnels



PrimeLink 5001 Desktop

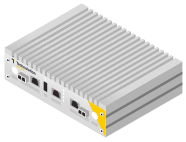
Is onderdeel van het netwerk in praktijkvoorbeeld 3.

PrimeLink 3015+ Desktop

Is onderdeel van het netwerk in praktijkvoorbeeld 2.

Product specificatie overzicht

19" variant

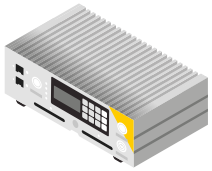


desktop variant

	PrimeLink 3015+
Rubriceringsniveau	Departementaal VERTROUWELIJK EU RESTRICTED (v1.0.4.0) NATO RESTRICTED Stg. CONFIDENTIEEL zonder APTs (v2.0.x.0)
Omgeving	TBB4 (Departementaal VERTROUWELIJK) TBB3 (Stg. CONFIDENTIEEL)
Netwerkconfiguratie	Point-to-point, hub-spoke, mesh
Aantal end-point tunnels	128
Aantal routes	128
Interfaces	Electrisch: 1 Gbit/s Optisch: 1 of 10 Gbit/s
LAN tunnels	L2 (Ethernet) L3 (IPv4)
WAN header	L4 (UDP over IPv4 over Ethernet)
Protocol	OpenVPN – UDP
Encryption	AES-256-GCM
Tunnel routing	Longest Prefix Matching destination IP (L3 mode) VLAN-ID (L2 mode)
Control channel bescherming	TLS-Crypt V2 authentication & encryption
Bandbreedte (per richting)	>990 Mb/s (9 KB packets; 1 Gbit/s mode) >9900 Mb/s (9 KB packets; 10 Gbit/s mode)
Packets/s (per richting)	>800.000 (64 byte packets; 1 Gbit/s mode) >8.000.000 (64 byte packets; 10 Gbit/s mode)
MTU	Jumbo frames: 12.000 bytes (WAN)
Monitoring	Online in-band Online out-band
Management	In-band Out-band Offline (CIK)
Latency	< 50µs unidirectioneel (< 0,05 ms)
Beheersysteem	Domain Administration Station (DAS)
Sleutelbron	Domain Administration Station (DAS)
Height	1U (19" variant) 1U (desktop variant)
Koeling	Passief

19" variant

19" variant



desktop variant

	PrimeLink 4010	PrimeLink 5001
	Stg. GEHEIM Stg. ZEER GEHEIM	Stg. CONFIDENTIEEL *(onder evaluatie)* Stg. GEHEIM Stg. ZEER GEHEIM EU TOP SECRET *(onder evaluatie)* NATO (COSMIC) TOP SECRET *(onder evaluatie)*
	TBB2 (Stg. GEHEIM) TBB1 (Stg. ZEER GEHEIM)	TBB3 (Stg. CONFIDENTIEEL *(onder evaluatie)*) TBB2 (Stg. GEHEIM) TBB1 (Stg. ZEER GEHEIM)
	Point-to-point	Point-to-point, hub-spoke, mesh
	1	120
	N.v.t.	2048
	Optisch: 10 Gbit/s	Optisch: 1 Gbit/s
	L2 (Ethernet)	L3 (IPv4)
	L2 (Ethernet)	L4 (UDP over IPv4 over Ethernet)
	Proprietary	Proprietary IKEv2 / IPsec - UDP
	NLNCSA proprietary (256 bits)	NLNCSA proprietary (256 bits)
	N.v.t.	Longest Prefix Matching on source VLAN-ID and destination IP address
	Proprietary (256 bits)	Closed User Group (256 bits)
	> 9900 Mb/s (9 KB packets)	>989 Mb/s (9 KB packets)
	>10.000.000 (64 byte packets)	>900.000 (64 byte packets)
	Jumbo frames: 12.000 bytes (WAN)	Jumbo frames: 12.000 bytes (WAN)
	Online out-band	Online in-band
	Offline out-band (management mode)	In-band
	< 50µs unidirectioneel (< 0,05 ms)	< 50µs unidirectioneel (< 0,05 ms)
	N.v.t.	PrimeLink 5000 Management Server (MS) PrimeLink 5000 Key Server (KS)
	NDA-SP (afdeling sleutelproductie van de NDA)	PrimeLink 5000 KS
	2U	1U (19" variant) 1U (desktop variant)
	Actief (vervangbare ventilatoren)	Passief

Services en **diensten**

De eindgebruikers in uw organisatie merken na implementatie niets van onze encryptie-oplossingen, maar onzichtbare beveiliging vraagt wel om goed beheer. Om te zorgen dat het systeem betrouwbaar en veilig blijft functioneren, bieden wij een compleet pakket aan services voor installatie, beheer en support.

Migratie- en installatiesupport
Overweegt u de invoering van High Assurance encryptie in uw organisatie? Wij denken actief met u mee over de optimale oplossing voor uw specifieke situatie. Vervolgens maken we samen met u een plan voor de installatie, de uitrol en het beheer. Daarbij streven we altijd naar minimale impact op de dagelijkse processen. Desgewenst voeren wij de volledige installatie van de encryptie-oplossing voor u uit. Hierbij nemen wij alle stappen van het proces voor onze rekening: de levering en fysieke installatie van de apparatuur, de configuratie, de commissioning (ingebruikname van de apparatuur) en het operationeel brengen van het netwerk.
U kunt er ook voor kiezen om (een deel van) deze stappen zelf uit te voeren.

Training en opleiding
Voor de medewerkers die onderhoud en beheer van de beveiligde netwerken binnen uw organisatie uitvoeren, bieden wij een complete set trainingen, verzorgd door onze High Assurance experts. Deze variëren van kortdurende hands-on trainingen voor het dagelijks netwerkbeheer, tot meerdaagse diepgaande theorietrainingen voor beveiligings-experts en (crypto)beheerders. De trainingen worden altijd afgestemd op uw specifieke behoeftes.

Support
Uiteraard kunt u ook na installatie en ingebruikname een beroep op ons doen voor hulp en ondersteuning bij storingen of incidenten. Hiervoor bieden we verschillende opties:

Standaard Ad Hoc Support

Incidentele hulp op afroep, op nacalculatie, zonder SLA of gegarandeerde reactietijden

Uitgebreide Support (8x5)

Afgesproken reactietijden binnen kantooruren, inclusief 60 uur support per jaar

Permanente Support (24x7)*

Afgesproken reactietijden 24x7, inclusief 60 uur support per jaar, voor kritieke systemen

Graag bespreken we met u de optimale supportmogelijkheden voor uw organisatie.

Services
Naast support bieden wij u ook de mogelijkheid om de beheertaken van uw netwerk geheel of gedeeltelijk aan ons over te dragen. Deze services bieden wij in twee varianten: Essential en Premium.

* Beschikbaar vanaf najaar 2026

Technolution
Prime

Essential Services
Voor laag- en hooggerubriceerde netwerken

Uw organisatie verzorgt in deze variant de eerstelijns-intake bij incidenten. Alle overige beheertaken nemen wij van u over, waaronder:

- **Commissioning** en installatie
- **Periodiek onderhoud** – denk aan het vernieuwen van sleutels en certificaten, het uitvoeren van firmware-updates of het vervangen van batterijen
- **Uitvoeren** van netwerkwijzigingen
- **Vervangen** van eventuele defecte apparatuur

Premium Services
Voor laaggerubriceerde netwerken met de PL3015+

Technolution verzorgt in deze variant zowel de eerstelijns-ondersteuning als de monitoring en het technisch beheer van uw encryptieoplossing.

- **Eerstelijnsbeheer** door Technolution op afstand
- **Proactieve monitoring** van uw netwerk door Technolution
- **Volledige ontzorging** van het technisch beheer (zie Essential Services)
- **In bewaring nemen en uitvoeren van periodieke back-ups** van het management-systeem (DAS)
- Potentiële **problemen worden geïdentificeerd en aangepakt** voordat ze escaleren

Services en diensten op maat
Voor alle services en diensten geldt: maatwerk is altijd mogelijk. Onze High Assurance experts helpen u graag om de encryptiebehoeftes van uw organisatie in kaart te brengen en een passende oplossing te vinden voor de services en diensten die u nodig hebt.

Technolution

Opgericht
1987

Technologiebedrijf

Multidisciplinair - software, elektronica en programmeerbare logica

- Oplossingen die ertoe doen
- Betrouwbare technologie
- Anders denken

300
Gedreven medewerkers

8,4
Medewerkers-tevredenheid

8,2
Klant-tevredenheid

75 mln.
Omzet

10-15%
Van de omzet R&D

28e
In NL top 30 R&D

Locaties

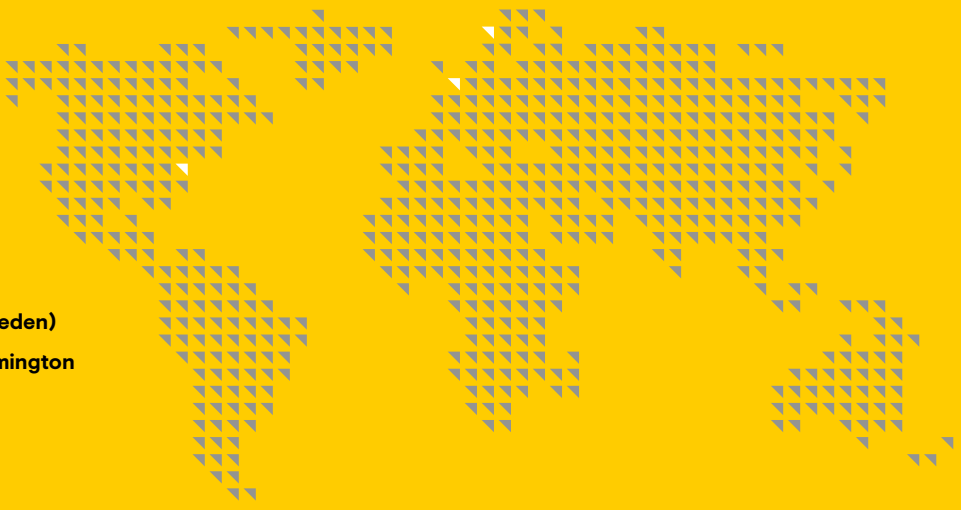
Technolution - **Gouda**

Technolution Deventer - **Deventer**

Phase to Phase - **Arnhem**

Technolution Nordics - **Stockholm (Zweden)**

TNL USA Inc. & TNL Nanotech Inc. - **Wilmington**



Submerken

Technolution Move

Technolution Advance

Technolution Prime

Technolution Spark

Certificeringen

ISO 9001 Kwaliteit

ISO 27001 Informatiebeveiliging

ISO 14001 Milieu

CO_2 prestatieladder niveau 5

COLOFON

ONTWERP, LAY-OUT EN INFOGRAPHICS
Studio Piraat, Den Haag

Redefining
solutions

11. 2025

Technolution
Prime

Over Technolution Prime

Technolution Prime is de koploper in Nederland in preventieve high assurance oplossingen voor gerubriceerde data. Wij ontwikkelen onze producten en oplossingen volledig in eigen huis. We staan voor hoogwaardige cyber security waar die het hardst nodig is.

Technolution
Burgemeester Jamessingel 1
2803 WV Gouda
Nederland

+31 (0)182 59 40 00
prime@technolution.com
technolution.com/prime
Technolution Prime

technolution.com/prime