Technolution
Prime

Network Encryption Solutions

Securely connecting classified networks

Redefining **solutions**

““Government networks are under constant attack by state actors. **High-end encryption is indispensable for our national security.** Our encryption solutions protect the government’s and citizens’ sensitive data from attackers.”

Jonathan Hofman
High Assurance Business Unit Director

Technolution
Prime

Contents

Secure connections in a changing world

The importance of reliable encryption for government organizations has never been greater. The geopolitical situation in the world has changed irreversibly. There is an invisible war going on in cyberspace and cyberattacks and digital espionage are now everyday realities.

The ICT infrastructure of government departments, agencies, and other government bodies is under constant attack. The attackers are often state actors: professional individuals and organizations that are supported by their countries and have almost unlimited resources at their disposal. In this digital arms race, encryption protects the confidentiality and integrity of sensitive information.

The strategic importance of encryption
High-end encryption is an indispensable part of our national security. Without robust encryption, government departments are at risk of having critical information intercepted or manipulated by foreign powers. Encryption protects international cooperation, diplomatic communications, and defense intelligence. But encryption is also important on the national level. It underwrites mutual trust between government and citizens.

Citizens expect their data to be securely stored, and government organizations need secure digital infrastructures to carry out their policies.

Secure connections, also in the future
The purpose of cyberattacks is often to access secret information through the external data connections of secure networks. Connections between multiple locations across an open, untrusted network like the internet are particularly vulnerable to attack. An attacker who gains access to a data connection can then penetrate the connected networks and intercept and decipher data.

PrimeLink network encryptors encrypt data before it is transmitted across a data connection, and decrypt it at the other end. The data is unreadable without the right encryption keys. The encryption method used is particularly important to safeguard maximum resistance against attack. With the arrival of quantum computers, encryption may not be totally safe anymore in the future, even with larger keys. This is why PrimeLinks use 'quantum-resistant' encryption methods; their encryption cannot be hacked even by a quantum computer.

Quantum resistance and post-quantum cryptography

In practice, quantum computers cannot yet be used for encryption. And yet quantum technology plays a big role in encryption, because quantum computers are theoretically much faster than binary computers. As soon as a quantum computer with sufficient 'qubits' is developed, many cryptographic algorithms will become vulnerable to hacking; according to estimates, this may happen at some point between 2030 and 2050.

Fortunately, there are encryption methods that can resist the power of the quantum computer, such as 256-bit, symmetrical quantum-resistant keys and post-quantum cryptography. Thanks to these methods, our PrimeLinks are prepared even today for future attacks by quantum computers.

Evaluated encryption for classified information
The Dutch intelligence agency AIVD's Unit Weerbaarheid (Resilience Unit) offers Dutch government bodies an overview of evaluated solutions for the protection of classified information. The Resilience Unit provides a usage advisory for each evaluated product, which specifies conditions and guidelines for using the products for each classification level, from NLD RESTRICTED up to and including NL TOP SECRET.

FPGAs – combining the security of hardware with the flexibility of software

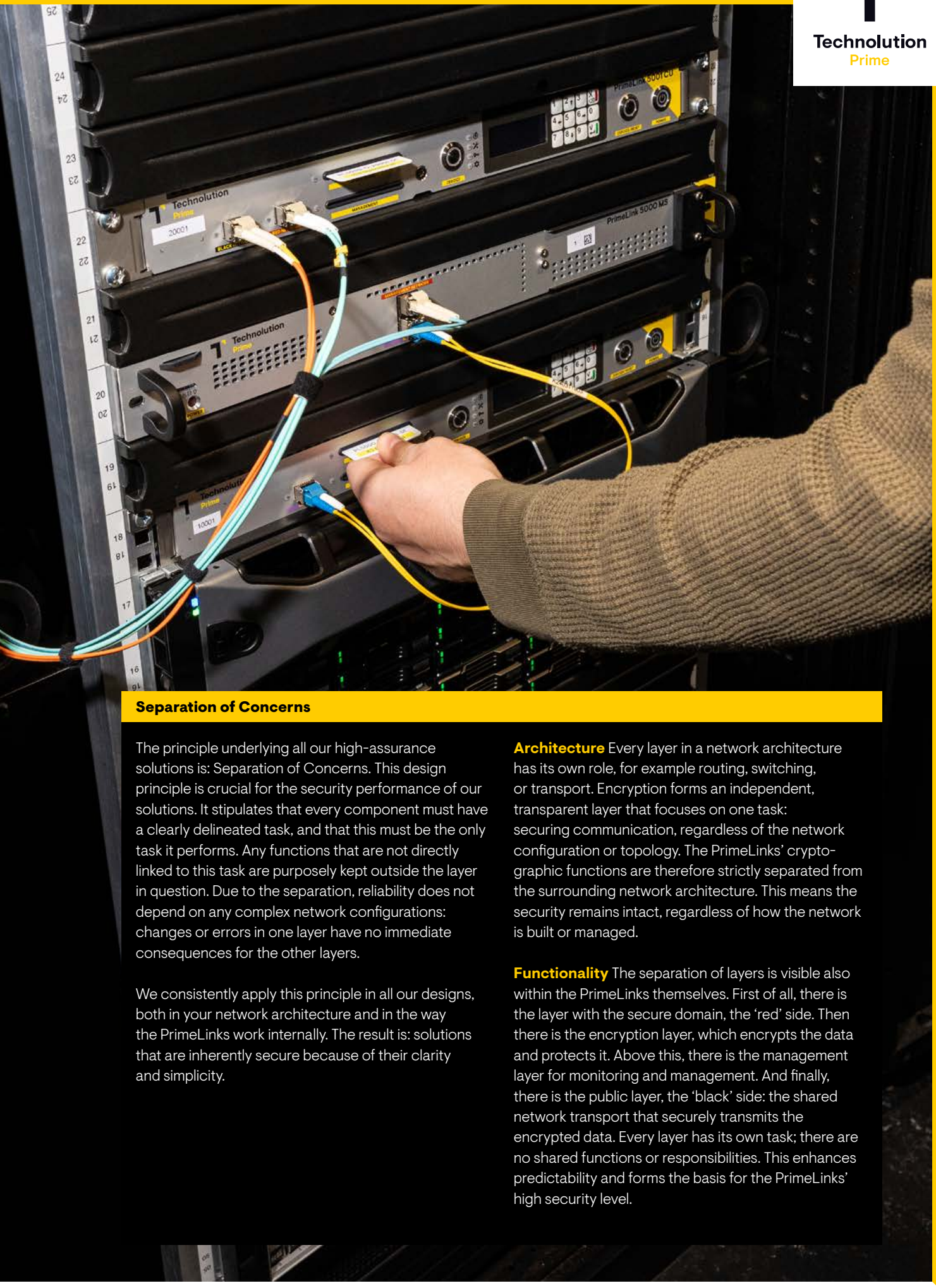
Our security products run internally with Field-Programmable Gate Arrays, or FPGAs. These programmable chips are fitted with firmware in a special language. They perform cryptographic algorithms in parallel, which makes them very fast and efficient and reduces the risk of interference between processes to a minimum. As cryptographic keys and processes are performed in separate logical blocks, FPGAs are highly secure. Keys are strictly shielded from any other components either within or outside the FPGA.

The great advantage of FPGAs is that they can be reprogrammed, for example to add new cryptographic standards, security updates, or functionalities. This means the functionality of the PrimeLinks can be renewed and adapted at all times. Updates may contain new features, such as a throughput speed of 10 Gbit/s instead of 1 Gbit/s, or a new cryptographic algorithm. In this way, network encryption grows with the user's needs and the latest requirements in the field of security. There is no need to replace the hardware to do this. FPGAs combine the reliability of hardware and the flexibility of software.

Technolution Prime's PrimeLink encryption solutions have all been evaluated by the Resilience Unit, which can also provide usage advisories upon request.

Technolution Prime's method
Technolution is market leader in the Netherlands in the field of evaluated encryption and domain separation. Under the brand name Technolution Prime, we develop and produce network encryptors, data diodes, data filters, and other high-assurance security products. 'Separation of concerns' is the guiding principle in all our products. In addition, we develop project-based tailormade solutions and offer support, cryptography management, and consultancy on security issues, particularly for government organizations.

For optimal flexibility and security, we use FPGAs, programmable (and reprogrammable) chips. This makes our Prime products fast, flexible, and future-proof – they are regularly updated with new functionalities or features.



Separation of Concerns

The principle underlying all our high-assurance solutions is: Separation of Concerns. This design principle is crucial for the security performance of our solutions. It stipulates that every component must have a clearly delineated task, and that this must be the only task it performs. Any functions that are not directly linked to this task are purposely kept outside the layer in question. Due to the separation, reliability does not depend on any complex network configurations: changes or errors in one layer have no immediate consequences for the other layers.

We consistently apply this principle in all our designs, both in your network architecture and in the way the PrimeLinks work internally. The result is: solutions that are inherently secure because of their clarity and simplicity.

Architecture Every layer in a network architecture has its own role, for example routing, switching, or transport. Encryption forms an independent, transparent layer that focuses on one task: securing communication, regardless of the network configuration or topology. The PrimeLinks' crypto-graphic functions are therefore strictly separated from the surrounding network architecture. This means the security remains intact, regardless of how the network is built or managed.

Functionality The separation of layers is visible also within the PrimeLinks themselves. First of all, there is the layer with the secure domain, the 'red' side. Then there is the encryption layer, which encrypts the data and protects it. Above this, there is the management layer for monitoring and management. And finally, there is the public layer, the 'black' side: the shared network transport that securely transmits the encrypted data. Every layer has its own task; there are no shared functions or responsibilities. This enhances predictability and forms the basis for the PrimeLinks' high security level.

PrimeLink

High-end, Dutch-made encryption

The defining features of our PrimeLink encryption products are their clear, effective functionality coupled with speed and flexibility. This is the result of our development philosophy of ‘separation of concerns’ and of our use of FPGAs: programmable chips. This powerful combination is the core of the Technolution Prime philosophy: clear architecture, maximum security, and adaptable functionality.

Reliability guaranteed
The reliability of our security solutions for government organizations must be conclusively proven. Very thorough testing, in combination with exhaustive documentation and evaluation by the AIVD’s Unit Weerbaarheid (Resilience Unit) are important steps in doing this.

Supply chain
Electronic components are often sourced in multiple countries – and not all of these are friendly states. This is why we have been very critical in selecting our main part suppliers in the supply chain. Moreover, we impose additional checks and requirements on our suppliers. This means you can be sure that your encryption device was built using safe components.

Assembly
We fully assemble our products ourselves to ensure reliability, applying the same strict norms we do during design. The work is done by screened staff at a separate, secure location that meets the high requirements set by the Dutch government. In this way we safeguard not only the technical quality, but also the confidentiality and integrity of each product.

Technolution
Prime

Technolution Prime's **encryption products**

PrimeLinks offer high-end, classified encryption made in the Netherlands.

PRIMELINK 3015+

Network encryptor for classification levels **NLD RESTRICTED** and **NLD CONFIDENTIAL**

- 1 *and* 10 Gbit/s, layer 2 *and* 3, quantum-resistant, Non-CCI
- Online monitoring and remote management
- Encrypted connection with OpenVPN software clients possible
- Suited for NLD CONFIDENTIAL from firmware v2.0.0.0 in situations without APTs (Advanced Persistent Threats)

PRIMELINK 4010

Line encryptor for classification levels **NLD SECRET** and **NLD TOP SECRET**

- 10 Gbit/s, high speed, maximum bandwidth at layer 2
- Minimal management burden
- Quantum-resistant

EU NATO
Under evaluation

PRIMELINK 5001

IP encryptor for **NLD SECRET** and **NLD TOP SECRET**

- 1 Gbit/s, layer 3, quantum-resistant
- User-friendly management, developed in close consultation with end users
- Optimized stock management and key plan for rapid implementation, smarter logistics
- Also available as PrimeLink 5001c for NLD CONFIDENTIAL

Encryption **ecosystems**

PrimeLink network encryptors work discreetly in your organization, supported by well-designed ecosystems for management and monitoring. These systems give your network administrators a firm grip on their network configurations. In addition, the systems provide clear insight into the performance of the encrypted connections.

PrimeLink 3015+

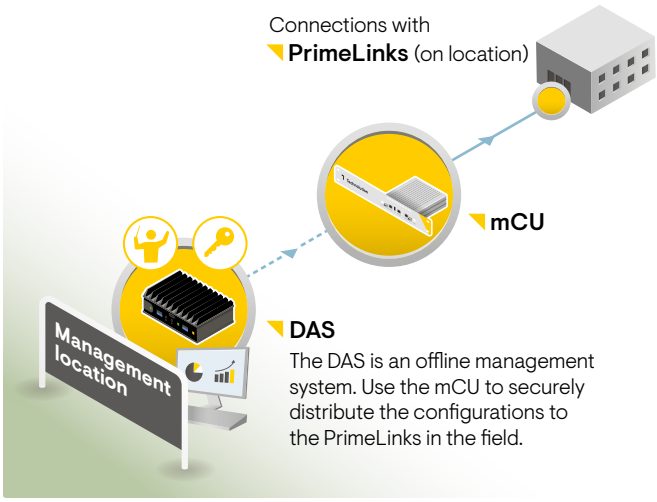
Central management using DAS

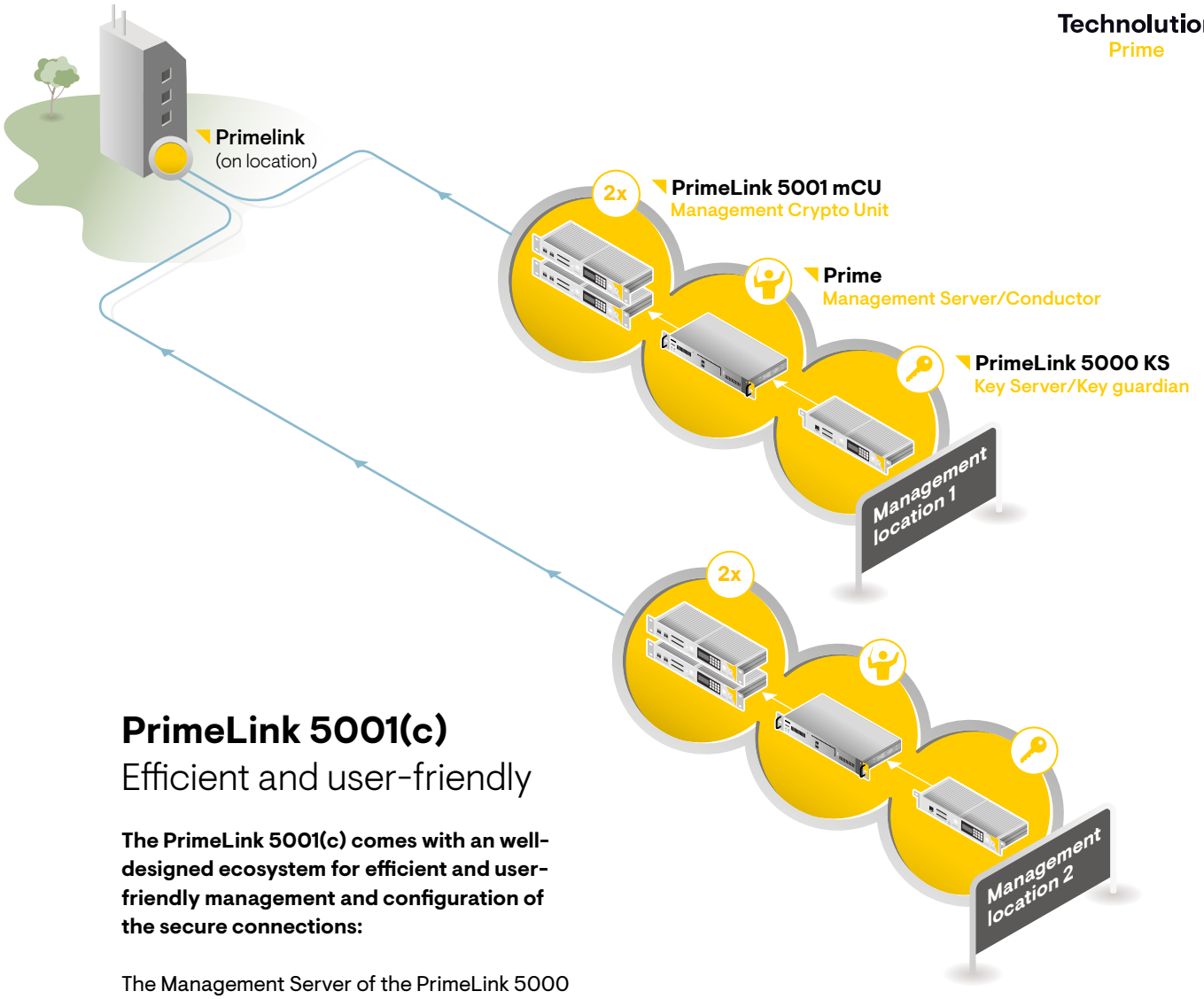
The Domain Administration Station stands at the heart of managing the PrimeLink 3015+.

The Domain Administration Station (DAS) is a special system that generates a unique configuration image for every PrimeLink 3015+ in a network domain. Administrators then distribute these images online through the Management Crypto Unit, or offline using USB sticks. A clear system of network domains and PrimeLink groups helps the network administrator to create, manage, and monitor a wide selection of secure network configurations.

- **Online** monitoring and management
- **Remote** updates
- **Hitless updates** – the network remains active (available from firmware v3.0.0.0)
- **One or more management locations** from which the network is managed

The PrimeLink 3015+ ecosystem	
Crypto Unit (CU)	The “connector”. The PrimeLink 3015+ Crypto Units that set up the secure connections for data traffic.
Domain Administration Station (DAS)	The “conductor” and the “key guardian”. An offline system that is the primary interface for management and monitoring. The DAS generates and keeps all keys, certificates, and configurations required for setting up secure connections between CUs.
Management Crypto Unit (mCU)	A CU that functions as a secure management connection between the DAS and the CUs in the network.





PrimeLink 5001(c)

Efficient and user-friendly

The PrimeLink 5001(c) comes with an well-designed ecosystem for efficient and user-friendly management and configuration of the secure connections:

The Management Server of the PrimeLink 5000 series offers a user-friendly graphical interface to create and manage network configurations. Administrators can create a secure network with just a few mouse clicks. Network configurations and IP routing tables are then generated automatically. The new network configuration can be easily distributed to all PrimeLinks in the network using the Management Crypto Unit.

- Easy **online management and configuration** due to unique user interface
- Easy **centralized stock management**
- Interaction with **National Distribution Authority** required only once
- After installation, **permanently manage and maintain your network yourself** thanks to optimized key plan

The PrimeLink 5001 (c) ecosystem	
Crypto Unit (CU)	The “connector”. The PrimeLink 5001(c) Crypto Units that set up the secure connections for data traffic.
Management Server (MS)	The “conductor”. Implements management and configuration of the CUs in the field and is the primary management interface.
Key Server	The “key guardian”. Generates the keys that are distributed through the MS and the Management CU to the CUs with the secure connections.
Management Crypto Unit (mCU)	A CU that functions as a secure management connection between the MS and the CUs in the network.

Encrypting connections

Network encryption **in practice**

What encryption solution is best suited for your organization?

This depends on several factors. Some of these are linked to what your organization does, such as your activities, how sensitive the information is that you handle, and the classification level. Other factors are technical, including the type of network, the number of secure connections, and the bandwidth required. Organizational aspects also play a role, such as the size and expertise of your management organization. We are happy to advise you on the best options for your specific situation.

The following pages showcase a number of illustrative examples.


Technolution
Prime

USE **CASE 1**

Secure point-to-point connections with high bandwidth

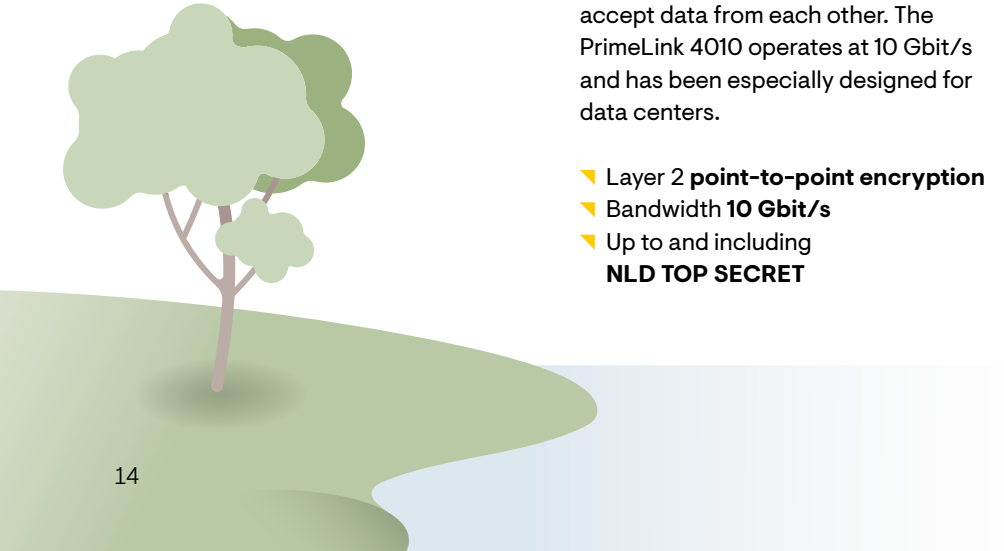
Datacenter **interconnectivity**

THE SITUATION

A data-intensive government organization works with highly classified information. It has two primary datacenters and a third datacenter for backup. Confidentiality and continuity are crucial. Everything stored in datacenter 1 is therefore synchronized in real time with datacenter 2. If datacenter 1 were to fail, datacenter 2 will immediately take over all tasks. The backup data center, no. 3, functions as a digital safety net. The data of the primary data centers is periodically offloaded there. In case of major calamities, such as failure of both primary data centers, all data of the organization will be restored from the backup data center.

THE CHALLENGE

The organization generates large data flows. Real-time synchronization between the primary data centers and offloading to the backup are effected through dedicated point-to-point connections. The bandwidth of the connections must be large enough to process all these flows of highly sensitive information. This requires rapid, low-latency encryption that meets the high classification requirements.



THE SOLUTION

The PrimeLink 4010 and the PrimeLink 3015+ (for NLD RESTRICTED) both offer sufficient bandwidth for the point-to-point connections between the data centers.

PrimeLink 4010

High speed, high classification levels, minimal management

The PrimeLink 4010 is always delivered as a pair. The two devices will only accept data from each other. The PrimeLink 4010 operates at 10 Gbit/s and has been especially designed for data centers.

- Layer 2 **point-to-point encryption**
- Bandwidth **10 Gbit/s**
- Up to and including **NLD TOP SECRET**

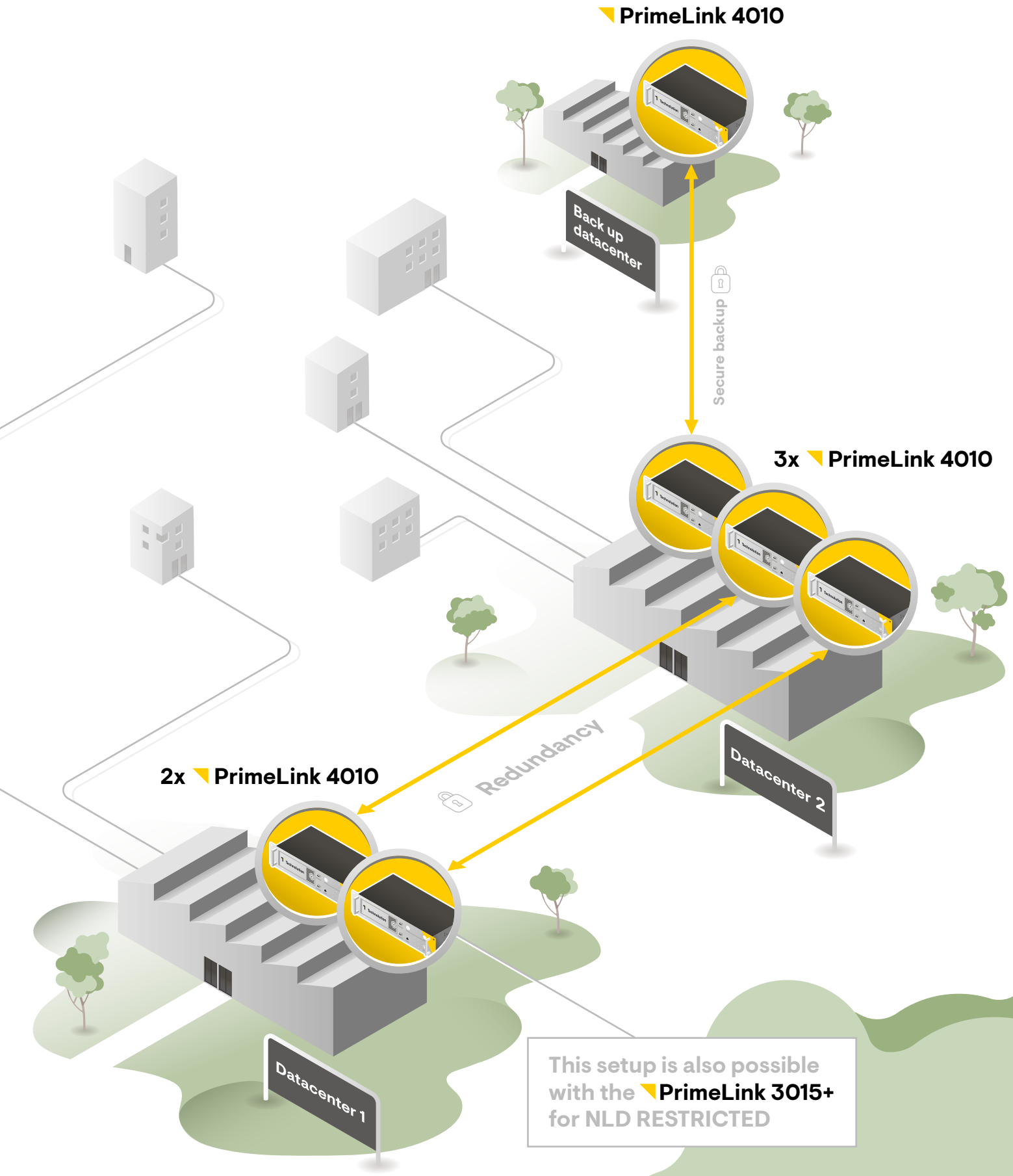
PrimeLink 3015+

Flexibility in speed and network options

The PrimeLink 3015+ offers 1G and 10G bandwidths, both in configuration with layer 2 point-to-point line encryption and in configuration with layer 3 IP-encryption. This network encryptor can therefore be used in almost all network configurations.

- Layer 2 **point-to-point encryption**
- Layer 3 **encryption for IP networks**
- Bandwidth **1 Gbit/s** or **10 Gbit/s**
- Up to and including **NLD RESTRICTED** or **NLD CONFIDENTIAL***

* From firmware v2.0.0.0, in situations without state actor threats



This setup is also possible with the PrimeLink 3015+ for NLD RESTRICTED

USE **CASE 2**

Maximum flexibility in network configurations

Encryption between government locations

THE SITUATION

The employees of this government organization work in a wide range of locations. The organization has offices across the country that all exchange data with each other. The information within the organization is classified as NLD RESTRICTED. The information has to be available at all times. Staff work with classified information, including when they work from home. For this, they need access to the network. Their work files are synchronized in real time and staff often download large files. Videocalls and remote access sessions similarly require a lot of bandwidth.

THE CHALLENGE

There are no dedicated connections between the locations; all connections of the network, including connections with people working from home, are across the internet. There is no need for an extremely large bandwidth, but scalability is required – both as regards bandwidth and the number of connections. The solution must be suited for the classification level NLD RESTRICTED and, in due course, for a full mesh network. Staff working from home need a solution that will have minimal impact on their home office, but that does offer a secure connection.

THE SOLUTION

PrimeLink 3015+

Post-quantum cryptography for NLD RESTRICTED

The data connections between locations are encrypted using the PrimeLink 3015+. This has been configured at layer 3 as hub and spoke. The configuration is flexible; a full mesh configuration, in which the network is fully enmeshed, is also possible. The PrimeLink 3015+ offers quantum resistance, has been certified for NLD RESTRICTED, and has a bandwidth of either 1 Gbit/s or 10 Gbit/s. Network updates are implemented without network interruptions.

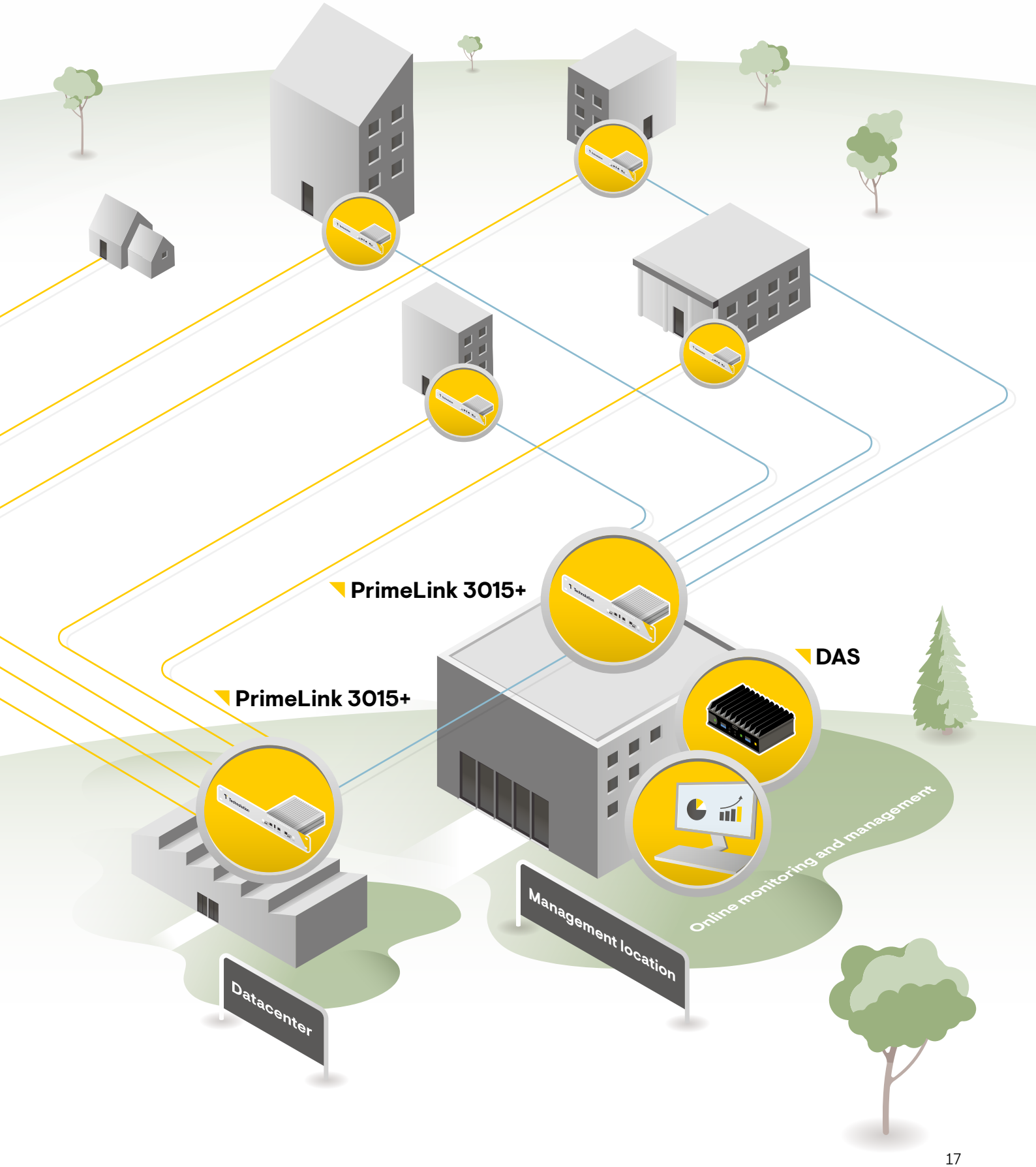
Staff working from home will have to install a software client on their computer that connects directly with a PrimeLink 3015+ in the organization network. This software client is compatible with the PrimeLink 3015+ but has a lower encryption speed. NB a software client installed on an employee's personal computer is inherently less safe than the hardware encryption of the PrimeLink 3015+. Additional measures are recommended.

Technolution
Prime

THE SOLUTION

Encrypted connections

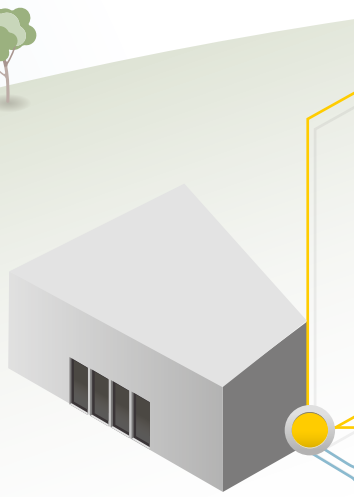
Management tunnels



USE **CASE 3**

Large-scale encryption for critical networks

Complex, large-scale, **highly classified networks**



THE SITUATION

A large government organization operates at a national level. The organization has offices and branches at hundreds of locations, which are all connected to each other in one large, partially meshed network. The organization works with extremely sensitive information, up to and including NLD TOP SECRET. Any hack of the communication lines of this organization, for example by a state actor, would result in serious problems.

THE CHALLENGE

Even though security is the first priority, a robust solution that can be managed easily is also an important requirement for this organization. High availability of the entire network (24/7) is essential. In addition, administrators must be able to quickly change or expand the network. The solution must be suited for the highest classification levels and resistant to future attacks with quantum computers.

THE SOLUTION

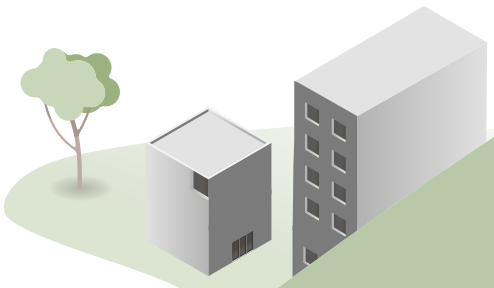
PrimeLink 5001

Robust, flexible, user-friendly

The locations of the organization are connected with each other through PrimeLink 5001 IP encryptors. These will be dedicated connections; the local networks will be linked directly across the internet with the PrimeLink 5001. PrimeLink 5001s only accept data from other PrimeLink 5001s that have been configured for this. Administrators can easily change the configuration in an intuitive, user-friendly management application, which gives oversight even over large networks.

Stock management and the key plan for the PrimeLink 5001 are optimally adjusted to the requirements of large organizations with decentralized infrastructures. Interaction with the National Distribution Authority is required only once, for the initial enrollment of the management environment. Afterwards, your organization can permanently manage and maintain the network itself.

- **NLD TOP SECRET**
- **Full mesh** and other configurations
- **Post-quantum** cryptography
- **Dual Power Supply**, suited for use in datacenters
- Centralized and decentralized management, optimized **stock management and key plan**

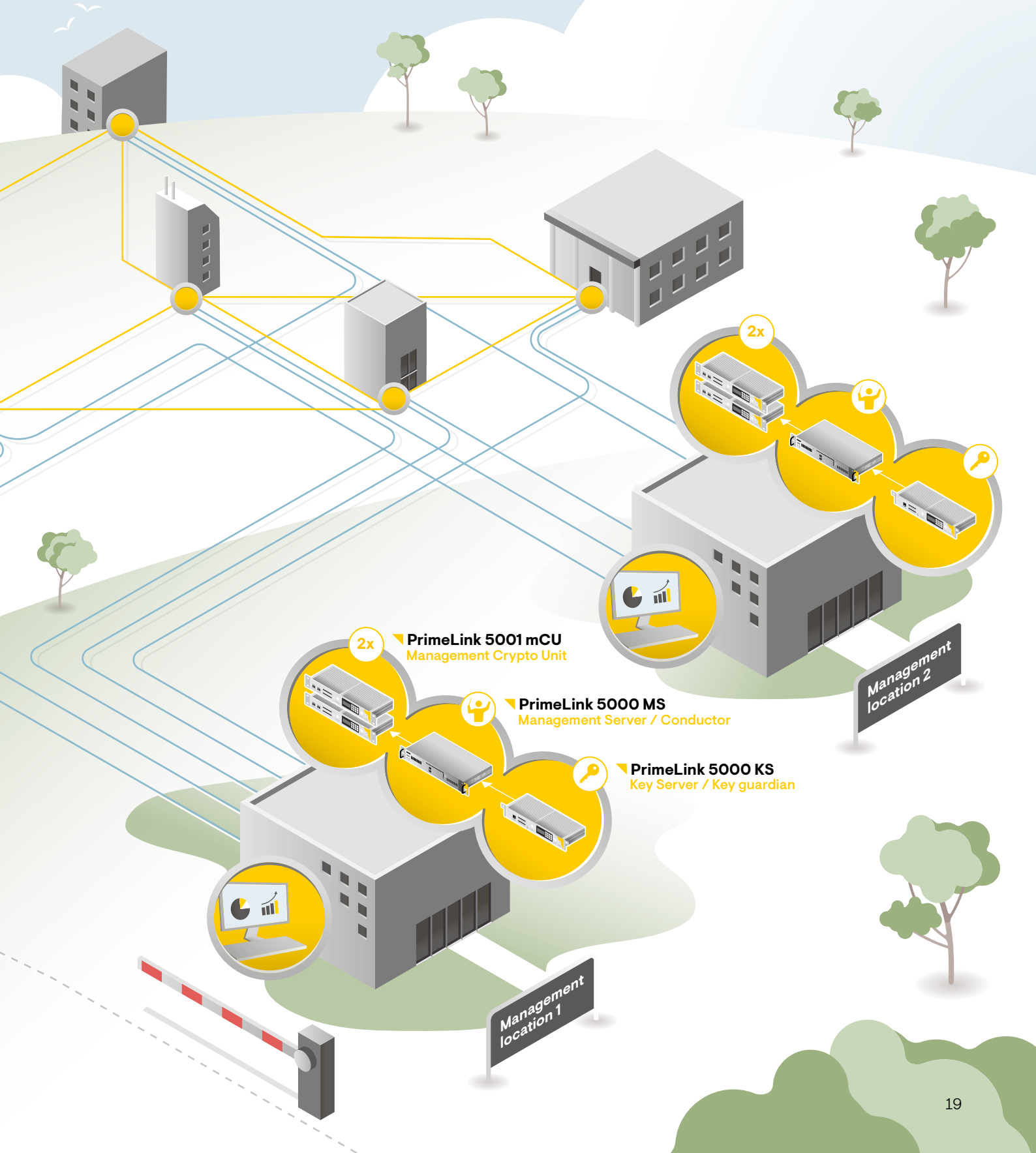


THE SOLUTION

Encrypted connections

Management tunnels

Primelink (on location)



USE **CASE 4**

High-assurance encryption in desktop format

Robust encryption for every location

THE SITUATION

A government organization maintains data connections with outposts in remote locations. Fast and reliable exchange of information is vital for staff in these outposts, but connections are unstable and of strongly varying bandwidths.

THE CHALLENGE

Due to the limited space in the outposts, there are no server racks for standard 19'' encryption devices there. The encrypted connection with head office ideally has a high bandwidth for rapid exchange of large volumes of information. In practice, the bandwidth varies per outpost. The encryption requirements also vary per outpost, but are all at least NLD RESTRICTED and often higher. Quantum resistance or post-quantum encryption is required, as is high reliability of the secure connection.

THE SOLUTION

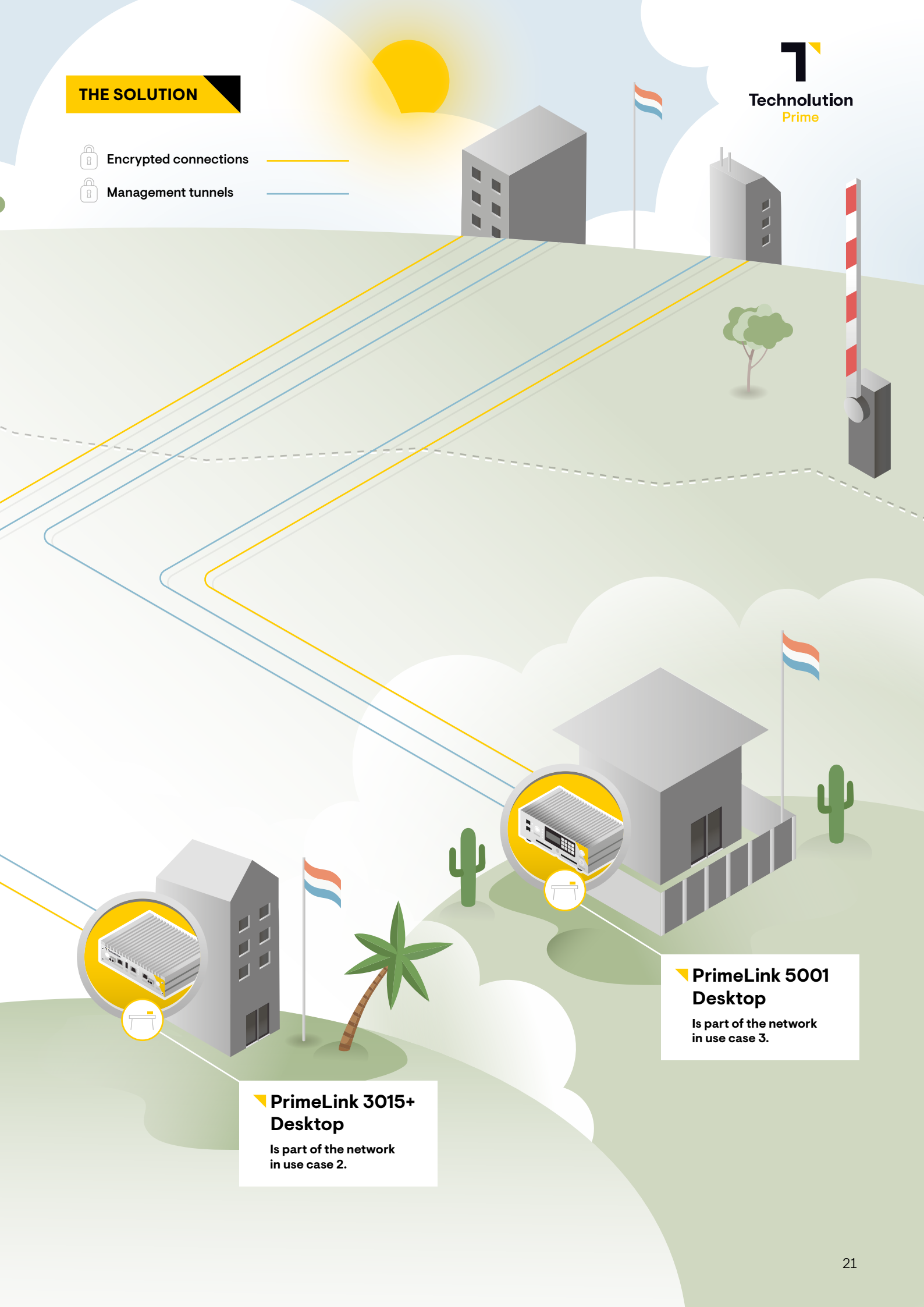
Desktop versions of PrimeLink 3015+ and PrimeLink 5001

High-assurance encryption without compromise

The desktop versions of PrimeLink 3015+ and PrimeLink 5001 offer post-quantum encryption with the required bandwidth for the classification levels NLD RESTRICTED and NLD SECRET/ NLD TOP SECRET respectively. These compact versions have been especially designed for locations where space, power supply, or IT infrastructure are limited.

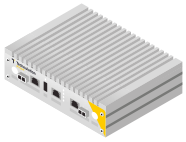
Despite their compact form, these PrimeLinks make no concessions on performance or specifications; these are almost identical to the larger 19'' versions. Both the PrimeLink 3015+ and the 5001 are suited for remote management. All desktop versions can function in a network that operates with varying bandwidths alongside each other.

- **Desktop model** with compact form factor
- Suited for almost **all network configurations**
- **Multiple bandwidths** at the same time
- **No concessions** on performance and security features


THE SOLUTION
Encrypted connections
Management tunnels
Technolution
Prime
PrimeLink 5001 Desktop
Is part of the network in use case 3.
PrimeLink 3015+ Desktop
Is part of the network in use case 2.

Product specifications

19" version

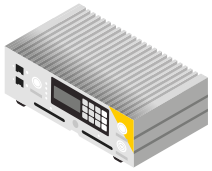


desktop version

	PrimeLink 3015+
Classification level	NLD RESTRICTED EU RESTRICTED (v1.0.4.0) NATO RESTRICTED NLD CONFIDENTIAL without APTs (v2.0.x.0)
Environment	TBB4 (NLD RESTRICTED) TBB3 (NLD CONFIDENTIAL)
Network configuration	Point-to-point, hub-spoke, mesh
Number of end-point tunnels	128
Number of routes	128
Interfaces	Electrical: 1 Gbit/s Optical: 1 or 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 protection	TLS-Crypt V2 authentication and encryption
Bandwidth (per direction)	>990 Mb/s (9 KB packets; 1 Gbit/s mode) >9900 Mb/s (9 KB packets; 10 Gbit/s mode)
Packets/s (per direction)	>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 unidirectional (< 0,05 ms)
Management system	Domain Administration Station (DAS)
Key source	Domain Administration Station (DAS)
Height	1U (19" version) 1U (desktop version)
Cooling	Passive

19" version

19" version



desktop version

	PrimeLink 4010	PrimeLink 5001
	◥ NLD SECRET ◥ NLD TOP SECRET	◥ NLD CONFIDENTIAL *(under evaluation)* ◥ NLD SECRET ◥ NLD TOP SECRET ◥ EU TOP SECRET (under evaluation) ◥ NATO (COSMIC) TOP SECRET (under evaluation)
	◥ TBB2 (NLD SECRET) ◥ TBB1 (NLD TOP SECRET)	◥ TBB3 (NLD CONFIDENTIAL *(under evaluation)*) ◥ TBB2 (NLD SECRET) ◥ TBB1 (NLD TOP SECRET)
	Point-to-point	Point-to-point, hub-spoke, mesh
	1	120
	N/a	2048
	Optical: 10 Gbit/s	Optical: 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/a	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 unidirectional (< 0,05 ms)	< 50µs unidirectional (< 0,05 ms)
	N/a	◥ PrimeLink 5000 Management Server (MS) ◥ PrimeLink 5000 Key Server (KS)
	NDA-SP (NDA's key production division)	PrimeLink 5000 KS
	2U	◥ 1U (19" version) ◥ 1u (desktop version)
	Active (replaceable ventilators)	Passive

Services

The end users in your organization won't even notice our encryption solutions once they have been implemented, but invisible security does require good management. To ensure that the system continues to function reliably and safely, we offer a complete suite of services for installation, management, and support.

Migration and installation support
Are you considering introducing high-assurance encryption in your organization? We are happy to talk with you about the optimal solution for your specific situation. The following step is that we draw up a plan, in consultation with you, about installation, rollout, and management. Our guiding principle is to reduce the impact on your daily business processes to a minimum. If necessary, we can take care of the full installation of the encryption solution for you. This means we perform all the steps involved: delivery and physical installation of the devices, configuration, commissioning of the devices, and making the network operational. You can also choose to do one or more of these steps yourself.

Training
Our high-assurance experts offer a complete range of training courses for the employees who will be responsible for service and management of the secure networks within your organization. These courses vary from short hands-on sessions for daily network management to multi-day, in-depth theoretical courses for security experts and crypto administrators. These training programs are always finetuned to meet your specific needs.

Support
Naturally you can also count on us for assistance and support in case of faults or incidents after installation and commissioning. We have various packages to choose from:

- **Standard Ad Hoc Support**

  Incidental on-demand assistance, based on subsequent calculation, without SLA or guaranteed response times

- **Extensive Support (8x5)**

  Agreed response times during office hours, including 60 hours of support per year

- **Permanent Support (24x7)***

  Agreed response times 24x7, including 60 hours of support per year, for critical systems

We are happy to discuss the best support options for your organization.

Services
In addition to support, we also offer the option of doing the management of your network for you, either in its entirety or in part. We have two packages: Essential and Premium.

* Available from late 2026.

Technolution
Prime

Essential Services
For networks involving both low and high classification levels

In this package, your organization is responsible for the primary intake in case of incidents. We will take care of all other management tasks, including

- **Commissioning** and installation
- **Periodic maintenance** – including key and certificate replacement, carrying out firmware updates, and replacing batteries
- **Performance** of network changes
- **Replacement** of any faulty devices

Premium Services
For networks involving low classification levels using the PrimeLink 3015+

In this package, Technolution takes care both of the primary support and of monitoring and technical management of your encryption solution.

- **Primary support**, remotely by Technolution
- **Proactive monitoring** of your network by Technolution
- We take **full charge of technical management** (see Essential Services)
- **Storage and performance of periodic backups** of the management system (DAS)
- **Identifying and solving potential problems** before they escalate

Tailormade services
All services can be offered as tailormade solutions. Our high-assurance experts are eager to help you map the encryption needs of your organization and offer a suitable solution for the service you need.

Technolution

Founded
1987

Technology company

Multi-disciplinary – software, electronics and programmable logic

- Solutions that matter
- Reliable technology
- Thinking differently

300
Motivated employees

8,4
Employee satisfaction

8,2
Customer satisfaction

75 mln.
Revenue

10-15%
Of revenue R&D

28th
In Dutch Top 30 R&D

Locations

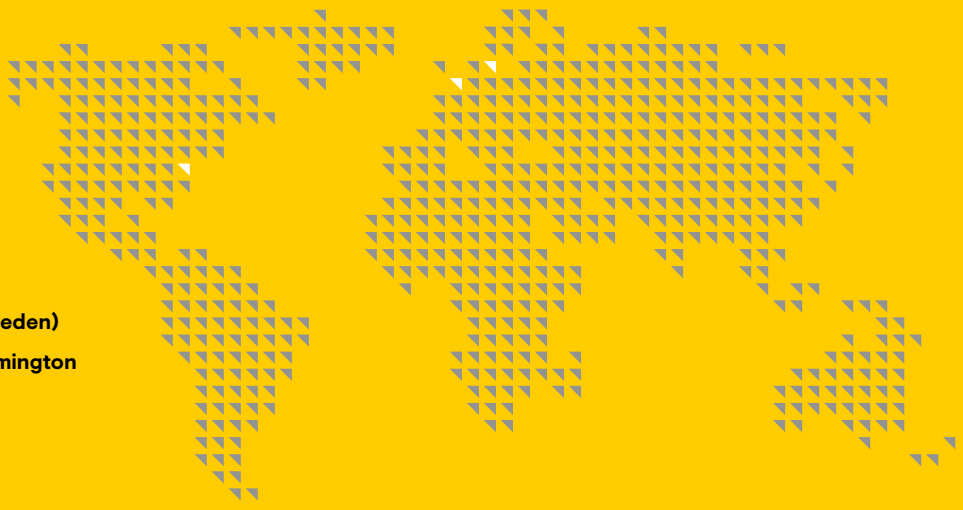
Technolution - **Gouda**

Technolution Deventer - **Deventer**

Phase to Phase - **Arnhem**

Technolution Nordics - **Stockholm (Sweden)**

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



Sub-brands

- Technolution Move
- Technolution Advance
- Technolution Prime
- Technolution Spark

Certifications

- **ISO 9001** Quality
- **ISO 27001** Information security
- **ISO 14001** Environment
- **CO_2** Performance Ladder level 5

COLOPHON

DESIGN, LAYOUT AND INFOGRAPHIC
Studio Piraat, The Hague

Redefining
solutions

11. 2025

Technolution
Prime

About Technolution Prime

Technolution Prime is market leader in the Netherlands for preventive high-assurance solutions for classified data. We provide high-end cybersecurity for organizations that need it most.

Technolution
Burgemeester Jamessingel 1
2803 WV Gouda
Netherlands

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

technolution.com/prime