Technical specifications

PrimeCross

SECURITY	
Certification	Unclassified up to NLD SECRET
Hardware protection	Tamper evident and tamper responsive
Tempest	NATO SDIP-27 Level B

FILTER	
Filter pipeline	Hardware-based filter pipeline consisting of multiple isolated stages. The pipeline validates if the data structure complies with predefined formats and allows certain recognized structures to be further analyzed by a flexible programmable processing engine.
Typical use-cases	Message structure validation, pattern matching, XML validation, XML element capturing and validation, message transformation, etc.
Filter policies	Secure loading of filter definitions for different message types
Data interface	Two interfacing options: 1. A library with an Open API for low-level direct interaction with the unit 2. Full integration with PrimeDocks for more complex protocol and filter pipelines

INTERFACES	
Data interfaces	Optical 1Gbps (1000Base-SX, Duplex-LC)
Management interface	Ethernet 1000Base-T (RJ45)
Logging interface	Ethernet 1000Base-T (RJ45)

INTEGRATED PROXY'S (shelter only)	
CPU	Intel i5 (x86-64) Intel® Core™ i5-8365UE, Quad Core, 6M Cache, 1.6GHz (4.1GHz)
Memory	4GB RAM
Storage	32GB SSD

HARDWARE	
Regularly compliance	CE, RoHS, REACH
Cooling	Active (integrated)
Weight	~10 kg
Dimensions	19" rack: 1 U, 500 mm deep
Temperatures Operating	Datacenter 10°C - 35°C ambient Shelter 0°C - 45°C ambient 5 - 90% relative humidity (non-condensing)

Over Technolution Prime

About Technolution Prime Technolution Prime is the leader in Netherlands in preventive high assurance solutions for classified data. We develop our products and solutions entirely in-house. We stand for high quality cyber security where it is needed most.

Technolution B.V.
Burgemeester Jamessingel 1
2803 WV Gouda
The Netherlands

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

Technolution Prime

PrimeCross

technolution.com/ prime

Cross-domain hardware filter for SECRET information

Redefining **solutions**

PrimeCross will achieve a long-awaited goal. It will automate the bidirectional exchange of classified information between network domains of different security levels. PrimeCross consists of a hardened, FPGA-based hardware core with customizable filter policies. It couples future-proof upgradeability with great flexibility. This highly adaptable platform is fit for military-grade use cases with high assurance security. PrimeCross is being developed in close cooperation with the Dutch Ministry of Defense and will be evaluated by the NLNCSA before release.

Photo: Mediacentrum Defensie

Check, filter and convert data
The PrimeCross offers a safe alternative for the data exchange with mobile data carriers such as USB sticks, or through software-based filters and firewalls. It provides a secure and hardened hardware environment, so that users can focus all their attention on creating application-specific filters (policies) between network domains with different security levels.

Fit for many use cases
With its features for the automated checking, filtering and converting of data, the PrimeCross accomodates for many different situations, applications and domains.

Secure, bidirectional exchange of **classified information**

Use Case 1: Checking Data Security Levels – Create filter policies for checking data security levels and blocking the transport of higher-security information to lower-security domains. Data of the appropriate level can be allowed to pass the filter.

Use Case 2: Linking Combat Simulations – Securely join combat vehicle simulations of different army units, such as fighter jet, ground vehicle, and navy ship simulations. Multiple countries within an alliance may even combine simulations through PrimeCross for joint international combat training.

Use Case 3: Converting Sensitive Data - When data need to be transformed, truncated, or removed before sharing them with a lower-security network domain, create a conversion filter to remove or change the relevant data accordingly. I.e. automatically reduce the accuracy of coordinates to prevent sharing precise positions of ground troops.

Use Case 4: Allowing software updates - Validate the signatures of software updates to allow for secure automated transfer of software updates to higher security domains.

Evaluated hardware
Since the FPGA-based hardware core of PrimeCross will come evaluated and ready to use, only the filter policies that you create will need evaluation before deployment. This greatly speeds up the process of creating new data links. In addition, development, management and maintenance of custom filter policies are performed by your own organization, which minimizes the risk of unwanted outside intervention. Technolution Prime offers expert services and advice for users and developers of filter policies.

PrimeDocks for proxy applications

When using PrimeCross for filtering data between network domains, supporting (proxy) applications on both sides of the PrimeCross are required. Before and after filtering, these proxies convert data to and from formats that are readable by the PrimeCross.

Technolution's PrimeDocks is an open platform that offers a flexible environment for developing and configuring the required proxies. Together, PrimeCross and PrimeDocks provide a complete toolbox for secure cross-domain data transfer.

Datacenter and Shelter
PrimeCross will come in two versions.

PrimeCross FD60 "Datacenter"

The PrimeCross FD60 "Datacenter" is a stand-alone cross-domain hardware filter in a 19" 1U casing. With configurable, firmware data filters, the FD60 is especially suited for processing large quantities of data. The FD60 works with external proxy servers, thus granting the best options for speed and bandwidth.

PrimeCross FS60 "Shelter"

The PrimeCross FS60 "Shelter" offers specifications similar to the FD60. However, with the FS60, proxy software can be installed directly on the embedded operating system. Thanks to this space-saving option the FS60 is especially suited for field deployment, i.e. in vehicles or mobile control centers.