KPN Security Policy

KSP – Standard

Title	**Network and Communication Security**	
ID	**KSP-FA05-ST03**	
Funct. Area	05 – System and Network security	
Date	2 November 2016	
Version	v2.6	
Status	Approved	
Owner	CISO	

Summary

The network and communication security policy describes the minimal set of requirements to facilitate the security and availability of networks and network services used to provide KPN services. This includes following networks (wired and wireless):
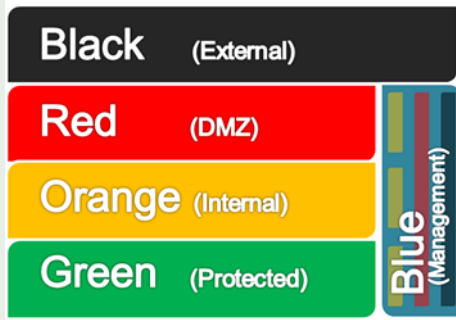- Internal transport networks;
- Management networks;
- Networking services for clients.

Version history

Version	Date	Comments
v1.0	20 August 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v2.0	15 April 2014	Update from organization feedback
v2.1	15 May 2014	Update based on review comments
v2.2	1 August 2014	Update based on consistency
v2.3	23 January 2015	Encrypted protocol use has changed from a must to a should. KSP-FA05-TL01 defines which traffic type is mandatory per zone.
v2.4	13 November 2015	Textual adjustments made based on annual review
v2.5	5 February 2016	Added explicit mention of KOEN wrt zoning
v2.6	2 November 2016	R03: Communication matrix added R06: STARTTLS and verified unencrypted patching added

Disclaimer

ID	KSP-FA05-ST03-R01
Title	Network segmentation and security zoning
Description	Segments must be defined and implemented for a network environment to support a layered security model. This can be achieved by building services in accordance to a security zoning model. The following is a high-level description of the KPN standard zoning model: A typical service would have the systems users (who are in the Black zone) need to interact with in the Red zone, systems that are purely for service internal use in the Orange zone and servers containing confidential data in the Green zone. All systems also need a connection into the Blue zone in order to be managed. The internal network KOEN is classified as a black zone.
Relating document	KSP-FA05-RL08 - Network Segmentation KSP-FA05-RL09 - WLAN Security
Rationale (why)	Just as in physical security, not everything happens in one room. Network segments should have a specific purpose and should be separated from other segments with their specific purpose. Segmentation must be done on function and classification of network data.
Example	A webserver that is used for serving webpages to internet should not be in the same segment as the backup system for this server.
Possible exception	N/A

ID	KSP-FA05-ST03-R02
Title	<u>Network filtering</u>
Description	Between network segments a network filter must be in place through which only necessary traffic can pass.
Relating document	KSP-FA05-RL08 - Network Segmentation
Rationale (why)	Network segments are defined because of their different uses, security wise and functionality wise. To keep these separated, filtering of networking traffic is necessary.
Example	A webserver may need a database server backend to be able to serve content to clients. This communication must be limited to only the necessary database communication to prevent misuse. This communication is registered in a communication matrix.
Possible exception	N/A

ID	KSP-FA05-ST03-R03
Title	Network documentation
Description	Network documentation must be present for network infrastructures describing: - The network design (including security requirements); - Required service levels; - IP number plan; - Communication matrix; - Dependency on external parties.
Relating document	N/A
Rationale (why)	This documentation is mostly needed for day to day management, but in case of a security incident this information can be used to assess the impact of an incident and facilitate in its solving.
Example	A network diagram showing how the network is built-up with a list of protocols needed for proper working of network and service delivery.
Possible exception	N/A

ID	KSP-FA05-ST03-R04
Title	<u>Network monitoring</u>
Description	Networks must be monitored for capacity, availability and malicious activities. Events must be handled as per the incident management process.
Relating document	KSP-FA05-RL06 - Logging and Monitoring
Rationale (why)	Monitoring is essential to be able to see what is happening on a network. Without monitoring, network management departments are "blind" and are not in control of a network.
Example	Monitoring a network link for over-usage or being able to detect a virus outbreak on the network.
Possible exception	N/A

ID	KSP-FA05-ST03-R05
Title	<u>Network availability</u>
Description	The design a network must ensure the required level of availability.
Relating document	N/A
Rationale (why)	Due to the function of a network component (handling traffic), different data streams for different services are transported. The highest availability requirement of the data streams prescribes the measures that must be taken for a network infrastructure.
Example	If a service must be "always on", robust components must be used and device- or location redundancy must be implemented.
Possible exception	N/A

ID	KSP-FA05-ST03-R06
Title	Encrypted protocols
Description	Encrypted protocols should be used when data is sent through the network. KSP-FA05-TL01 defines per traffic type and zone combination if encryption is mandatory.
Relating document	KSP-FA05-RL07 - Cryptography KSP-FA05-TL01 - Protocol and Port Usage KSP-FA05-TL02 - Cryptographic Algorithms and Cipher Suites
Rationale (why)	Network traffic can be intercepted. Whether it's in a green, orange or red zone; It's not possible to guarantee that traffic will not be intercepted. For this reason the use of secure protocols is mandatory in most cases.
Example	FTP is a protocol that can be used to transfer data. SCP or SecureFTP are secure alternatives for this. Standard unencrypted LDAP is not allowed however, when TLS is enforced by STARTTLS then it is allowed.
Possible exception	For some traffic or protocols there is no safe alternative. Additional measures must be taken to reduce the risk of information leakage. Known exceptions are: - High volume traffic where encrypting poses an insurmountable problem. - Systems communicating unencrypted public data, like updates, between verified peers. A KSP compliant method of detecting tampering with data has to be in place. - Systems communicating in the same VLAN (not spanning more than one building).