

KPN Security Policy



KSP – Rule

Title	WLAN security	<pre>graph TD; A[Top level policy (mandatory)] --> B[Standards (mandatory)]; B --> C[Rules (mandatory)]; C --> D[Guidelines (supporting)]; D --> E[Tools (supporting)];</pre>
ID	KSP-FA05-RL09	
Funct. Area	05 - System and Network security	
Date	2 November 2016	
Version	v1.4	
Status	Approved	
Owner	CISO	

Summary

Purpose of this document is to provide a minimum policy on WLAN (Wireless Local Area Network). This is intended as an addition to the rules already provided for access management and network segregation (FA05 ST03, ST05, RL02 and RL08) and focuses on the additional challenges with wireless access security.

These rules do not apply to services.

Note that the practical limitations between WLAN security and ease of use and economic feasibility made us assume the following ground rule as fact:

- Availability of a WLAN network cannot be guaranteed.

Version history

Version	Date	Comments
v1.0	1 October 2013	Approved in SSM
v1.1	11 October 2013	Updated based on consistency check
v1.2	23 January 2015	Updated based on feedback about wireless interception. Now states explicitly what you must use to prevent eavesdropping.
v1.3	13 November 2015	Denial of Service protection (R01) updated to actively prevent problems in wireless networks.
v1.4	2 November 2016	R03: expanded R05: removed

Disclaimer

The content of this document is to describe KPN's policy on this specific topic. If and when this document is partly or fully disclosed to parties outside of KPN, it's important to hereby note towards those parties that this contains KPN's intended policy and cannot in any way be read or construed to be an explicit or implied formal guarantee or promise that its content can always be fully executed or complied to.

ID	KSP-FA05-RL09-R01
Title	<u>Denial of Service protection</u>
Description	<p>The wireless network must protect itself and its clients from attacks like:</p> <ul style="list-style-type: none"> • Man in the Middle attacks • Spoofed services, e.g. <ul style="list-style-type: none"> ○ Gateways ○ DNS servers ○ DHCP servers ○ Provisioning servers ○ Proxy servers ○ Radius servers • Rogue access points, i.e. base stations actively mimicking a KPN network identified by a spoofed base station identifier or logical name. E.g. KPN, KOEN_mobile and KOEN_Wlan.
Relating document	N/A

ID	KSP-FA05-RL09-R02
Title	<u>Communication Security</u>
Description	<p>To prevent data across a WLAN from interception at least one of the following measure must be taken:</p> <ul style="list-style-type: none"> - Encrypt communication between client and access point using WPA2-Enterprise with 802.1x authenticated clients to the KPN MijnWerkplek WLAN. - Encrypt communication using a VPN solution offered by KPN MijnWerkplek.
Relating document	<p>Example of implementation with windows: Microsoft's guide - Windows firewall and IPSEC Policy deployment guide (http://technet.microsoft.com/library/cc732400.aspx) KSP-FA05-RL07-Cryptography</p>

ID	KSP-FA05-RL09-R03
Title	<u>WLAN configuration and connectivity</u>
Description	<p>When implementing a WLAN the following must be used:</p> <ul style="list-style-type: none"> - KPN WLAN with large user base (for example KPN Office Network) <ul style="list-style-type: none"> ○ use wpa2-enterprise ○ KPN managed client device must validate the authentication server based on certificate. ○ Users may access the KPN Office Network after authentication only when offered over the SSID KOEN_Wlan managed by KPN MijnWerkplek. - KPN WLAN with small user base, dedicated or personal scope: <ul style="list-style-type: none"> ○ must be secured with WPA2 with minimal key of 12 characters ○ Distribute and keep access keys conform private key requirements in KSP-FA05-RL07-R05 and R06 ○ The accessed network must be segmented from the KPN Office Network - KPN CPE WLAN for business and residential: <ul style="list-style-type: none"> ○ must be secured with WPA2 with minimal key of 10 characters initially ○ The accessed network must be the on premise network of the customer
Relating document	<p>Example of implementation with windows: Microsoft's guide - Configure PEAP and EAP methods: http://technet.microsoft.com/en-us/library/cc784383(v=WS.10).aspx</p> <p>Client validation settings enforcement: http://technet.microsoft.com/en-us/library/cc759575(v=ws.10).aspx#cert_based</p> <p>KSP-FA05-ST05 - Office Network and Office Automation</p> <p>KSP-FA05-RL07 - Cryptography</p>

ID	KSP-FA05-RL09-R04
Title	<u>WLAN access point management</u>
Description	The management interface of the wireless access points must not be available from the wireless part of the network.
Relating document	N/A