

Overview of selected KPN Security Policies

Creation date: Wednesday, December 4, 2019 1:35:34 PM

Selected by: Ruud Leurs

Requirement	WiFi Protected Setup
Description	No form of use of Wifi Protected Setup (WPS) is allowed.
ID	KSP-RE-420
Version	1.0
Date	December 11, 2017
Rationale	WLAN security

Requirement	WLAN configuration and connectivity
Description	<p>When implementing a WLAN the following must be used:</p> <p>KPN WLAN with large user base (for example KPN Office Network)</p> <p>use wpa2-enterprise</p> <p>KPN managed client device must validate the authentication server based on certificate</p> <p>Users may access the KPN Office Network after authentication only when offered over the SSID KOEN_Wlan managed by KPN MijnWerkplek</p> <p>KPN WLAN with small user base, dedicated or personal scope:</p> <p>must be secured with WPA2 with minimal key of 16 characters</p> <p>distribute and keep access keys conform private key requirements</p> <p>the accessed network must be segmented from the KPN Office Network</p> <p>KPN CPE WLAN for business and residential:</p> <p>must be secured with WPA2 with minimal key of 16 characters initially</p> <p>the accessed network must be the on premise network of the customer</p>
Related info	<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>
ID	KSP-RE-421
Version	1.1
Date	August 16, 2018
Rationale	WLAN security
Rationale	Security testing to innovation and development

Rationale	Authentication
Rationale	System hardening
Rationale	Registration of assets
Rationale	Cleaning of storage media
Rationale	Encrypting network traffic
Rationale	Data protection
Rationale	Cryptography generic
Rationale	Reporting security incidents

Requirement	WiFi Direct
Description	No form of use of Wifi-Direct is allowed.
ID	KSP-RE-419
Version	1.0
Date	December 11, 2017
Rationale	WLAN security

Requirement	Wireless connectivity to control and maintain objects
Description	<p>It is forbidden to control or maintain any object used for services, service components, or applications using any type of wireless connectivity past the stepping stone (i.e. wireless connectivity is allowed upto the stepping stone, after the stepping stone the connection must be wired).</p> <p>Examples of forbidden wireless connectivity is:</p> <p>Wi-Fi</p> <p>Bluetooth</p> <p>Infra-red</p> <p>Mobile network</p> <p>Other radio-based solutions using any type of antenna</p> <p>NFC-based solution with a maximum usage of 20 centimeters or less from (virtual) card to reader is allowed.</p>
Supplement	Radio based control and maintenance is susceptible to security, safety and continuity risks due to electro-magnetic disturbances and unable to control the object, man-in-the-middle attacks, circumvention of physical (access) controls and barriers due to radio leakage through walls.
ID	KSP-RE-754
Version	1.1
Date	August 9, 2019
Rationale	WLAN security
Rationale	Separating environments