Thursday, August 30, 2018 3:49:53 PM
Ruud Leurs

Requirement	**Application of cryptographic rules**
Description	All technology involving cryptography used in any network protocols, e.g. TLS-based (SMTP, FTP, HTTPS), SSH, EAP, IPsec and security of means (disk encryption, Hardware Security Modules, certificates) must adhere to the cryptography requirements of the KPN Security Policy. The scope includes, and is not limited to: - confidentiality techniques, e.g. encryption and pseudonimity - integrity control, e.g. Message Authentication Code (MAC) and one-way hash techniques - key exchange and key transport methods, e.g. forward secrecy and key exchange techniques - key storage quality, hardware security module quality - cryptographic processing norms, e.g. ETSI, FIPS, etc - proofs and non-repudiation techniques, like fingerprints and digital signatures, PKI and Web-of-Trusts as foundation to other systems including identity systems. - Quality in randomization techniques with specific focus towards cryptographic fundamental techniques.
ID	KSP-RE-410
Version	1.0
Date	December 11, 2017
Rationale	Encrypting network traffic

Requirement	**DNS namespacing for certificates**
Description	Internally and externally trusted certificates must use Subject Alternative Names (SANs) of the type DNS and Common Name fields (CNs) containing registered Fully Qualified Domain Names (FQDNs) with a registration to KPN as owner. For internally trusted certificates, the registration can be omitted when the Top Level Domain (TLD) ".local" is used.
ID	KSP-RE-411
Version	1.0
Date	December 11, 2017
Rationale	Encrypting network traffic

Requirement	**No internally trusted certificates for customers**
Description	Customer owned Fully Qualified Domain Names must not be signed by KPN internally trusted certificates, e.g. KPN N.V. Workspaces Root CA or KPN N.V. Private Root CA.
ID	KSP-RE-412
Version	1.0
Date	December 11, 2017
Rationale	Encrypting network traffic

Requirement	**Protecting data by encryption and digital signature techniques**
Description	Data transport of customer data, anykind of credential, internal data, confidential data and secret data must be protected by using protocols that ensure confidentiality, message integrity and authenticity between users and systems, and also machine to machine interaction. The transport of public files, system update files or packages, CRLs, CMPv2 are not considered confidential, thus encrypted protocols are not required for the security of the platform. Inbound data must be integrity protected by itself using a digital signature scheme to ensure the authenticity of the data and to ensure against tampering of the data before use. Systems using a STARTTLS protocol version, like XMPP with explicit TLS, FTP, SMTP, must enforce that credential and data exchange only occurs after both parties established a TLS handshake. Exception: Mail Transfer Agents who communicate to MTAs outside of KPN may deviate from this policy on advise from CISO. KSP-GL-513 defines per traffic type and zone combination if encryption is mandatory.
Supplement	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. 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 or when a LDAP discovery is started to be followed up by an encrypted data enchange. 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).
ID	KSP-RE-405

Version	1.1
Date	August 16, 2018
Rationale	Encrypting network traffic
Rationale	Cryptography generic

Requirement	**Forbidden protocols**
Description	The following protocols are forbidden to be used for any reason: SMBv1, RSH, SNMPv1, REXEC, NFSv1.
ID	KSP-RE-406
Version	1.0
Date	December 11, 2017
Rationale	Encrypting network traffic

Requirement	**Secure access**
Description	All connections between KPN End user devices (Endpoints) and devices such as printers and KPN corporate networks must be secured.
Supplement	To protect KPN End user devices, infrastructure and information against illegitimate, unauthorized (remote) access, and to secure remote connectivity from the Endpoint to the KPN infrastructure. Use encrypted communication and two factor authorization (such as the company card) for remote access of laptops.
ID	KSP-RE-407
Version	1.0
Date	December 11, 2017
Rationale	Encrypting network traffic

Requirement	**Communication Security**
Description	To prevent data across a WLAN from interception at least one of the following measure must be taken: - 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.
Related info	Example of implementation with windows: Microsoft’s guide - Windows firewall and IPSEC Policy deployment guide (http://technet.microsoft.com/library/cc732400.aspx)
ID	KSP-RE-408
Version	1.0
Date	December 11, 2017
Rationale	Encrypting network traffic
Rationale	Cryptography generic

Requirement	**Certificate Transparency**
Description	Any certificates used for internet-facing systems that are signed by a central CA must be registered in a Certificate Transparency repository.
ID	KSP-RE-409
Version	1.0
Date	December 11, 2017
Rationale	Encrypting network traffic