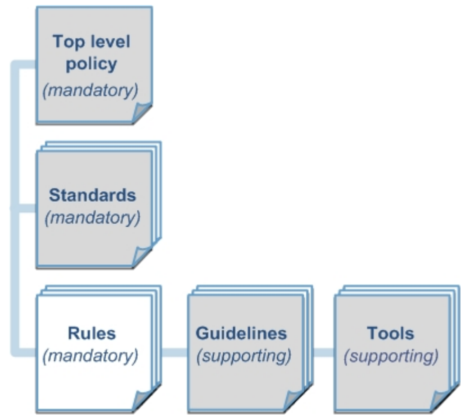
# KPN Security Policy

## KSP – Rule

| | | |
|---|---|---|
| Title | **Cryptography** |  Top level policy<br>(mandatory)<br>Standards<br>(mandatory)<br>Rules<br>(mandatory)<br>Guidelines<br>(supporting)<br>Tools<br>(supporting) |
| ID | **KSP-FA05-RL07** | |
| Funct. Area | FA05 – System and Network Security | |
| Date | 31 March 2014 | |
| Version | v2.0 | |
| Status | Approved | |
| Owner | CISO | |

### Summary

This document describes the requirements for all cases of encrypted communication, signed communication, use of PKI certificates, and use and management of encryption keys.

This document excludes requirements for when to use cryptography as those are described in other parts of the policy and those parts will refer to this document for the how-to.

### Version history

| *Version* | *Date* | *Comments* |
|---|---|---|
| v1.0 | 17 September 2013 | Approved in SSM |
| v1.1 | 11 October 2013 | Update based on consistency check |
| v2.0 | 31 March 2014 | Update based on use of policy and changes due to recent developments. |

*The latest version of this document can be downloaded from TEAMKPN*
*Any other version is uncontrolled.*

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R01 |
| **Title** | Cryptographic Key Generation, Random Bit Generator |
| **Description** | For each key used:<br>- When creating cryptographic keys the RBG (Random Bit Generator) of the product used must be compliant with one of the following standards:<br>○ [SP 800-90A]<br>○ [ANSI X9.62:2005, Annex D]<br>- Use of EC_Dual_DRBG is forbidden. |
| **Relating document** | http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R02 |
| **Title** | Cryptographic Key Generation, Cryptographic Module |
| **Description** | For each key used:<br>- When creating cryptographic keys the Cryptography Module of the product used must be compliant with the FIPS-140-2 standard. |
| **Relating document** | http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R03 |
| **Title** | Registration of Key Pair properties |
| **Description** | For each public/private key pair the following must be registered:<br>- The owner<br>- The intended use (infrastructure on which deployed)<br>- Key length<br>- Key Algorithm (including curve if Elliptic Curve is used)<br>- Hash<br>- CA used for signing<br>- Serial number (if applicable, like for certificates) |
| **Relating document** | |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R04 |
| **Title** | Key Pair privacy |
| **Description** | They private part of the key must be kept private by the owner. To support this:<br>- Key pairs must be generated locally by the key-pair owner or a delegated party within KPN (like Trusted Services or IT OPS).<br>- Certificate signing request must be submitted by CSR (Certificate Signing Request). |
| **Relating document** | CSR: http://en.wikipedia.org/wiki/Certificate_signing_request<br>KSP-FA05-RL07-R06 – Private Key transport and storage |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R05 |
| **Title** | Key Compromise |
| **Description** | Compromised keys must be rekeyed not updated. During generation the new key must be generated from a new set of data (no re-use of data used to generate the compromised key) to ensure its full independence from the compromised key. For PKI the CA must be informed of the compromise by means of the contract manager. |
| **Relating document** | N/A |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R06 |
| **Title** | Private key transport and storage |
| **Description** | For private key transport and storage:<br>- It must be impossible to determine the use and value of the plaintext key.<br>- Physical security steps must be taken to limit access to the key to authorized personnel. Any form of physical security in addition to building access, that allows verification of access (see point below) will do.<br>- If a stored key is accessed this must be verifiable/detectable. |
| **Relating document** | N/A |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R07 |
| **Title** | Public Key Exchange |
| **Description** | When public keys are shared the following two requirements must be adhered to:<br>- To prevent identity spoofing the exchange procedure used must ensure that the recipient of the public key is able to verify that the received key belongs to the owner of the private key.<br>- Similarly steps must be taken to ensure the integrity of the key shared during transfer. |
| **Relating document** | Key exchange mechanisms (http://en.wikipedia.org/wiki/Key_exchange) |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R08 |
| **Title** | Certificate Authority |
| **Description** | Certificate Authorities must be used that:<br>- Comply with the European Telecommunications Standards Institute (ETSI) standard "ETSI TS 101 456”<br>- Are FIPS 140-2 level 3 compliant or better.<br>- Have a published CPS (Certification Practice Statement), this also means that our use of the certificate must follow the CPS. |
| **Relating document** | ETSI:<br>http://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.04.03_60/ts_101456v010403p.pdf<br>FIIPS:<br>http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R09 |
| **Title** | Certificates |
| **Description** | Certificates must be used that comply with:<br>- RFC5280, in particular path validation and revocation checks<br>- Domain validation when used for identification. |
| **Relating document** | http://tools.ietf.org/html/rfc5280 |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R10 |
| **Title** | Use of certificates |
| **Description** | The certificate and the applications in which they are used must support the relevant RFC extensions describing use of certificates in combination with application or transport protocols. (For instance: RFC2818, to bind the identity of a peer to a session). |
| **Relating document** | Some much used examples include:<br>http://tools.ietf.org/html/rfc2818<br>http://tools.ietf.org/html/rfc2595 |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R11 |
| **Title** | Binding Certificates |
| **Description** | Each certificate must be bound to use for only one identity (for instance one host, Virtual Machine, one service or person or department).<br>An SSL off-loader or load-balancer MAY hold the certificate and private key to serve/off-load the SSL sessions for one cluster of nodes serving the same service. |
| **Relating document** | N/A |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R12 |
| **Title** | Wildcard Certificates |
| **Description** | Wildcard certificates must be scoped to the most specific subdomain possible and are not allowed directly under the first subdomain. This will limit impact in case of compromise. (Example: *.webmail.cm.kpn.com is better than *.cm.kpn.com for the consumer market webmail servers and *.kpn.com is never allowed.) |
| **Relating document** | http://en.wikipedia.org/wiki/Wildcard_certificate<br>KSP-FA05-RL07-R04 (key pair privacy) |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R13 |
| **Title** | Key pair lifetimes |
| **Description** | Key pairs used must have a maximum lifetime of 36 months. Maximum lifetime can be inherent, like with certificates, or managed by a key management process.<br>Exception to this is the key pairs used by a Certificate Authority. |
| **Relating document** | https://cabforum.org/Baseline_Requirements_V1_1_6.pdf |

| ID | KSP-FA05-RL07-R14 |
|---|---|
| **Title** | Encryption Algorithms |
| **Description** | One of the following encryption algorithms must be used:<br>- Three-key Triple DES Encryption and Decryption<br>- AES-128 Encryption and Decryption<br>- AES-192 Encryption and Decryption<br>- AES-256 Encryption and Decryption |
| **Relating document** | http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R15 |
| **Title** | Digital Signatures Algorithms |
| **Description** | One of the following digital signature algorithms must be used:<br>- DSA<br>- ECDSA<br>- RSA |
| **Relating document** | |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R16 |
| **Title** | Digital Signature Generation and Verification |
| **Description** | Digital signatures must have at least 112 bits of security strength. This means:<br>- For DSA: key length ≥ 2048 and hash length ≥ 224<br>- For RSA: key length ≥ 2048<br>- For EC: key length ≥ 224 |
| **Relating document** | |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R17 |
| **Title** | Key Agreement |
| **Description** | For Key agreement one of the following must be used:<br>- DH (Diffie-Hellman)<br>- MQV (Menezes-Qu-Vanstone)<br>- For both key length = 2048 and hash length is 224 or 256. |
| **Relating document** | |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R18 |
| **Title** | Hash Algorithms |
| **Description** | One of the following Hash Algorithms must be used:<br>- SHA-256<br>- SHA-384<br>- SHA-512<br>- SHA-1: for Non-digital signature generation applications only, not for Digital signature verification nor Digital signature generation after 2013<br>- SHA-224: for Non-digital signature generation applications only, not for Digital signature verification nor Digital signature generation after 2014 |
| **Relating document** | |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R19 |
| **Title** | HMAC (Hash-based Message Authentication Code) |
| **Description** | The following HMAC must be used:<br>- SHA-256 or better |
| **Relating document** | http://csrc.nist.gov/publications/nistpubs/800-107-rev1/sp800-107-rev1.pdf |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R20 |
| **Title** | SALT use |
| **Description** | The length of the randomly-generated portion of the salt must be at least 128 bits. |
| **Relating document** | N/A |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R21 |
| **Title** | Mixed Content |
| **Description** | To ensure the proper level of trust with a recipient there must not by any mixed content (mixing of unencrypted and encrypted content) when encrypting communication. This includes encrypted web pages. |
| **Relating document** | https://developer.mozilla.org/en-US/docs/Security/MixedContent |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R22 |
| **Title** | Maximum token lifetime |
| **Description** | Authentication tickets/tokens, e.g. Kerberos, AFS and Windows logon, must have a maximum lifetime of 6 hours. During their period of validity tokens may be refreshed automatically. |
| **Relating document** | N/A |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R23 |
| **Title** | Web application data encryption |
| **Description** | For encryption of web traffic use:<br>- TLS 1.2 |
| **Relating document** | http://tools.ietf.org/html/rfc5246 |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R24 |
| **Title** | Use Perfect Forward Secrecy |
| **Description** | Perfect Forward Secrecy must be used when setting up encrypted connections with any of the following protocols:<br>- IPSEC (Internet Protocol Security)<br>- SSH (Secure Shell)<br>- TLS (Transport Layer Security for web traffic)<br>- OTR (Off-The-Record messaging for instant messaging) |
| **Relating document** | http://en.wikipedia.org/wiki/Forward_secrecy |

| | |
|---|---|
| **ID** | KSP-FA05-RL07-R25 |
| **Title** | Use of multi-domain certificates |
| **Description** | Certificates must be scoped to only one application. The application may use multiple FQDNs (Fully Qualified Domain Names) to be identified. The FQDNs must share the same domain name.<br>Example:<br>• "www.kpn.com" and "kpn.com" can be combined<br>• "www.kpn.com" and "kpninternational.com" can not be combined<br>• "reporting.kpn.com" and "www.kpn.com" and "kpn.com" may be combined in one certificate when the "reporting" hostname is explicitly part of the overall application. |
| **Relating document** | Not Applicable. |