KPN Security Policy

KSP – Rule

Titel	**Cryptografie**
ID	**KSP-FA05-RL07**
FA	05 – Systeem- en netwerkbeveiliging
Datum	31 maart 2014
Versie	V2.0
Status	Goedgekeurd
Eigenaar	CISO

Samenvatting

In dit document worden de vereisten beschreven voor versleutelde communicatie, ondertekende communicatie, gebruik van PKI-certificaten, en gebruik en beheer van encryptiesleutels.

Dit document bevat geen vereisten over wanneer versleuteling moet worden toegepast, aangezien dat wordt beschreven in andere delen van de KSP. In die delen wordt naar dit document verwezen voor praktische instructies.

Versie-overzicht

Versie	*Datum*	*Opmerkingen*
v1.0	17 september 2013	Goedgekeurd tijdens SSM
v1.1	11 oktober 2013	Bijgewerkt op basis van consistentiecontrole
V2.0	31 maart 2014	Q1 policy update

De meest recente versie van dit document kan worden gedownload op TeamKPN.
Alle andere versies zijn niet geautoriseerd.

ID	KSP-FA05-RL07-R01
Titel	Generatie van encryptiesleutels; Random Bit Generator

Omschrijving	Voor iedere gebruikte sleutel geldt het volgende:
	- bij het creëren van encryptiesleutels moet de RBG (Random Bit Generator) van het gebruikte product voldoen aan een van de volgende standaarden:
	  ○ SP 800-90A;
	  ○ Bijlage D van ANSI X9.62:2005.
	- Gebruik van EC_Dual_DRBG is niet toegestaan

Gerelateerde documenten	NIST Special Publication 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators

ID	KSP-FA05-RL07-R02
Titel	Generatie van encryptiesleutels; encryptiemodule
Omschrijving	Voor iedere gebruikte sleutel geldt het volgende: - bij het creëren van encryptiesleutels moet de encryptiemodule van het gebruikte product voldoen aan de standaard FIPS-140-2.
Gerelateerde documenten	FIPS PUB 140-2: Security Requirements for Cryptographic Modules

ID	KSP-FA05-RL07-R03
Titel	Registratie van eigenschappen van sleutelparen
Omschrijving	Voor ieder publiek/geheim sleutelpaar moeten de volgende zaken worden geregistreerd: - de eigenaar; - het beoogde gebruik (de infrastructuur waarop de sleutel moet worden toegepast); - de lengte van de sleutel; - het algoritme van de sleutel (inclusief de curve indien gebruik wordt gemaakt van EC-cryptografie); - de hashfunctie; - de certificaatautoriteit (CA) die wordt gebruikt voor het ondertekenen); - het serienummer (indien van toepassing, bijvoorbeeld voor certificaten).
Gerelateerde documenten	

ID	KSP-FA05-RL07-R04
Titel	Vertrouwelijkheid van sleutelparen
Omschrijving	Het geheime gedeelte van de sleutel moet door de eigenaar geheim worden gehouden. Dit moet als volgt worden ondersteund: - sleutelparen moeten lokaal worden gegenereerd door de eigenaar van het sleutelpaar of door een gedelegeerde partij binnen KPN (zoals Trusted Services of IT OPS); - het verzoek om het certificaat te ondertekenen, moet worden ingediend door middel van het Certificate Signing Request (CSR).
Gerelateerde documenten	Wikipedia: Certificate Signing Request (http://en.wikipedia.org/wiki/Certificate_signing_request) KSP-FA05-RL07-R06 (Transport en opslag van geheime sleutels)

ID	KSP-FA05-RL07-R05
Titel	Gecompromitteerde sleutels
Omschrijving	Gecompromitteerde sleutels moet worden hersleuteld en niet worden bijgewerkt. Bij het hersleutelen moet de nieuwe sleutel worden gegenereerd uit een nieuwe gegevensset zodat hij volledig onafhankelijk is van de gecompromitteerde sleutel. Gegevens die zijn gebruikt om de gecompromitteerde sleutel te genereren, mogen dus niet opnieuw worden gebruikt. Bij PKI moet de certificaatautoriteit door de contractbeheerder worden geïnformeerd over de compromittering.
Gerelateerde documenten	Niet van toepassing

ID	KSP-FA05-RL07-R06
Titel	Transport en opslag van geheime sleutels
Omschrijving	Voor het transport en de opslag van geheime sleutels gelden de volgende bepalingen. - Het moet onmogelijk zijn om het gebruik en de waarde van de platte-tekst-sleutel te bepalen. - Er moeten stappen voor fysieke beveiliging worden ondernomen om toegang tot de sleutel te beperken tot geautoriseerd personeel; daarbij volstaat elke vorm van fysieke beveiliging (naast toegang tot het gebouw zelf) waarmee toegang kan worden gecontroleerd (zie het volgende punt). - Toegang tot opgeslagen sleutels moet verifieerbaar en opspoorbaar zijn.
Gerelateerde documenten	Niet van toepassing

ID	KSP-FA05-RL07-R07
Titel	Uitwisseling van publieke sleutels
Omschrijving	Wanneer publieke sleutels worden gedeeld, moeten de volgende twee vereisten in acht worden genomen. - Om *spoofing* van identiteiten te voorkomen, moet de gebruikte uitwisselingsprocedure ervoor zorgen dat de ontvanger van de publieke sleutel kan nagaan dat de ontvangen sleutel bij de eigenaar van de geheime sleutel hoort. - Ook moeten er stappen worden genomen om de integriteit te verzekeren van de sleutel die gedurende de overdracht wordt gedeeld.
Gerelateerde documenten	Wikipedia: Key Exchange (Engels) (http://en.wikipedia.org/wiki/Key_exchange)

ID	KSP-FA05-RL07-R08
Titel	Certificaatautoriteit (CA)
Omschrijving	De certificaatautoriteiten waarvan gebruik wordt gemaakt, moeten: - voldoen aan de standaard ETSI TS 101 456 van het European Telecommunications Standards Institute (ETSI); - voldoen aan Niveau 3 of hoger van de standaard FIPS 140-2; - beschikken over een gepubliceerd CPS (Certification Practice Statement) (dat houdt in dat ons gebruik van het certificaat het CPS moet volgen).
Gerelateerde documenten	ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates (http://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.04.03_60/ts_101456v010403p.pdf) FIPS 140-2: Security Requirements for Cryptographic Modules (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

ID	KSP-FA05-RL07-R09
Titel	Certificaten
Omschrijving	De certificaten waarvan gebruik wordt gemaakt, moeten: - voldoen aan de standaard RFC 5280, met name op het gebied van padvalidatie en revocatiecontroles; - gebruik maken van domeinvalidatie wanneer ze voor identificatie worden gebruikt.
Gerelateerde documenten	RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

ID	KSP-FA05-RL07-R10
Titel	Gebruik van certificaten
Omschrijving	Certificaten en de toepassingen waarin ze worden gebruikt, moeten de relevante RFC-standaarden ondersteunen waarin het gebruik van het certificaat wordt beschreven in combinatie met applicatie- of transportprotocollen (bijvoorbeeld: RFC 2818, om de identiteit van een *peer* aan een sessie vast te koppelen).
Gerelateerde documenten	Een paar veelgebruikte voorbeelden zijn onder meer: RFC 2818: HTTP Over TLS RFC 2595: Using TLS with IMAP, POP3 and ACAP

ID	KSP-FA05-RL07-R11
Titel	Vastkoppelen van certificaten
Omschrijving	Elk certificaat moet zijn vastgekoppeld om slechts voor één identiteit te kunnen worden gebruikt (bijvoorbeeld één host, virtuele machine, dienst, persoon of afdeling). Het is wel mogelijk dat een SSL-offloader of -loadbalancer het certificaat en de geheime sleutel aanhoudt om de SSL-sessies te verzorgen/offloaden voor één cluster nodes die dezelfde dienst verzorgen.
Gerelateerde documenten	Niet van toepassing

ID	KSP-FA05-RL07-R12
Titel	Wildcard-certificaten
Omschrijving	Wildcard-certificaten moeten zo specifiek mogelijk worden toegesneden op sub domeinen en zijn niet toegestaan direct onder het eerste sub domein. Dit om de gevolgen in geval van compromittering te beperken. (voorbeeld: *.webmail.cm.kpn.com beter dan *.cm.kpn.com voor de consumenten markt webmail servers en is *.kpn.com nooit toegestaan).
Gerelateerde documenten	Wikipedia: wildcard-certificaat (http://en.wikipedia.org/wiki/Wildcard_certificate) KSP-FA05-RL07-R04 (Vertrouwelijkheid van sleutelparen)

ID	KSP-FA05-RL07-R13
Titel	Levensduur van sleutelparen
Omschrijving	Gebruikte sleutelparen mogen een maximale levensduur van 36 maanden hebben. De maximale levensduur kan (net als bij certificaten) inherent zijn, maar kan ook worden beheerd met behulp van een sleutelbeheerproces. Sleutelparen die door een certificaatautoriteit worden gebruikt, zijn hiervan uitgezonderd.
Gerelateerde documenten	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

ID	KSP-FA05-RL07-R14
Titel	Encryptie-algoritmes
Omschrijving	Er moet een van de volgende encryptie-algoritmes worden gebruikt: - versleuteling en ontsleuteling met behulp van het 3DES-algoritme met drie sleutels; - versleuteling en ontsleuteling met behulp van het 128-bits AES-algoritme; - versleuteling en ontsleuteling met behulp van het 192-bits AES-algoritme; - versleuteling en ontsleuteling met behulp van het 256-bits AES-algoritme.
Gerelateerde documenten	NIST Special Publication 800-131A: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

ID	KSP-FA05-RL07-R15
Titel	Algoritmes voor digitale handtekeningen
Omschrijving	Er moet een van de volgende algoritmes voor digitale handtekeningen worden gebruikt: - het DSA-algoritme; - het ECDSA-algoritme; - het RSA-algoritme.
Gerelateerde documenten	

ID	KSP-FA05-RL07-R16
Titel	Generatie en verificatie van digitale handtekeningen
Omschrijving	Digitale handtekeningen moeten een beveiligingssterkte van ten minste 112 bits hebben. Dit wil zeggen: - voor het DSA-algoritme moet de sleutel ten minste 2.048 bits omvatten en de hashfunctie ten minste 224 bits; - voor het RSA-algoritme moet de sleutel ten minste 2.048 bits omvatten; - voor het ECDSA-algoritme moet de sleutel ten minste 224 bits omvatten.
Gerelateerde documenten	

ID	KSP-FA05-RL07-R17
Titel	Overeenkomen van sleutels
Omschrijving	Voor het overeenkomen van sleutels moet een van de volgende methodes worden gebruikt: - het DH-protocol (Diffie-Hellman); - het MQV-protocol (Menezes-Qu-Vanstone). - Voor beide geldt dat de sleutel 2.048 bits moet omvatten en de hashfunctie 224 of 256 bits.
Gerelateerde documenten	

ID	KSP-FA05-RL07-R18
Titel	Hash-algoritmes
Omschrijving	Er moet een van de volgende hash-algoritmes worden gebruikt: - het SHA-2-algoritme met 256 bits; - het SHA-2-algoritme met 384 bits; - het SHA-2-algoritme met 512 bits; - het SHA-1-algoritme (alleen voor toepassingen die geen digitale handtekeningen genereren; niet voor verificatie of generatie van digitale handtekeningen na 2013). - het SHA-2-algoritme met 224 bits (alleen voor toepassingen die geen digitale handtekeningen genereren; niet voor verificatie of generatie van digitale handtekeningen na 2014).
Gerelateerde documenten	

ID	KSP-FA05-RL07-R19
Titel	HMAC (Hash-based Message Authentication Code)
Omschrijving	De volgende HMAC moet worden gebruikt: - het SHA-2-algoritme met 256 bits of meer.
Gerelateerde documenten	Niet van toepassing

ID	KSP-FA05-RL07-R20
Titel	Gebruik van de saltfunctie
Omschrijving	De lengte van het willekeurig gegenereerde deel van de saltfunctie moet ten minste 128 bits zijn.
Gerelateerde documenten	Niet van toepassing

ID	KSP-FA05-RL07-R21
Titel	Combineren van versleutelde en niet-versleutelde informatie
Omschrijving	Om te zorgen voor het juiste vertrouwensniveau bij een ontvanger, mag er bij het versleutelen van communicatie geen versleutelde en niet-versleutelde informatie worden gecombineerd. Dit geldt ook voor versleutelde webpagina's.
Gerelateerde documenten	Mozilla Developer Network: Mixed Content

ID	KSP-FA05-RL07-R22
Titel	Maximale levensduur van tokens
Omschrijving	Authenticatietickets en -tokens (bijvoorbeeld het inlogprotocol van Windows, AFS of Kerberos) mogen een maximale levensduur van zes uur hebben. Tijdens hun geldigheidstermijn kunnen tokens automatisch worden vernieuwd.
Gerelateerde documenten	Niet van toepassing

ID	KSP-FA05-RL07-R23
Titel	Web applicatie data versleuteling
Omschrijving	Voor het versleutelen van web verkeer moet het volgende protocol gebruikt worden: - TLS 1.2
Gerelateerde documenten	http://tools.ietf.org/html/rfc5246

ID	KSP-FA05-RL07-R24
Titel	Gebruik Perfect Forward Secrecy
Omschrijving	Perfect Forward Secrecy moet gebruikt worden bij het opzetten van versleutelde verbindingen via een van de volgende methodes: - IPSEC (Internet Protocol Security) - SSH (Secure Shell) - TLS (Transport Layer Security) - OTR (Off-The-Record voor instant messaging)
Gerelateerde documenten	http://nl.wikipedia.org/wiki/Perfect_forward_secrecy

ID	KSP-FA05-RL07-R25
Titel	Gebruik van certificaten voor meerdere domeinen
Omschrijving	Certificaten moeten worden toegesneden naar slechts 1 applicatie. De applicatie mag meerdere FQDNs (Fully Qualified Domain Names of volledig uitgeschreven domein namen) gebruiken om zichzelf te identificeren. De verschillende FQDNs moeten binnen hetzelfde domein vallen. Voorbeelden: • "www.kpn.com" en "kpn.com" mogen gecombineerd worden. • "www.kpn.com" en "kpninternational.com" mogen niet gecombineerd worden • "rapportage.kpn.com" en "www.kpn.com" en "kpn.com" mogen gecombineerd worden mits de “rapportage” machine naam specifiek deel uitmaakt van de bovenliggende applicatie.
Gerelateerde documenten	Niet van toepassing.