Overview of selected KPN Security Policies

Creation date: Wednesday, December 4, 2019 1:38:10 PM

Selected by: Ruud Leurs

Requirement	**Web application data encryption**
Description	For encryption of transported application data applications: The highest available TLS version must be enabled. Protection against downgrade attacks must be activated. When this feature is absent: TLSv1.0 must be de-activated. TLSv1.3 must be enabled, when available. TLSv1.2 must be enabled. TLSv1.1 may only be enabled when there is a need to be able to communicate with legacy systems. When this need is absent, it must be disabled. TLSv1.0 may only be enabled when there is a need to be able to communicate with legacy systems. When this need is absent, it must be disabled. SSLv3 is not allowed to be enabled and must be completely disabled. SSLv2 is not allowed to be enabled and must be completely disabled. Enterprise TLS, as standardised by ETSI, is not allowed and must be completely disabled.
Related info	TLS 1.2 standard TLS 1.3 standard Enterprise TLS standard
ID	KSP-RE-487
Version	1.2
Date	May 3, 2019
Rationale	Cryptography generic

Requirement	**Retrieving content from remote locations**
Description	If content is retrieved from remote locations (over the internet) then always communicate through HTTPS, even if the content does not contain any personal/sensitive information.
ID	KSP-RE-350
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Web and Mobile Applications**
Description	Web applications running on systems reachable from the internet and mobile applications running directly on a mobile device must comply to the (Web) Application Security respectively Mobile App Security rule. The Portal Authority must give approval on first launch or on launch after a substantial change.
ID	KSP-RE-351
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**File upload**
Description	The upload functionality of an application or system must be hardened to prevent the execution of code or a denial-of-service situation.
ID	KSP-RE-352
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Rate limiting**
Description	Employ rate limiting and throttling on a per-user/IP basis (if user identification is available) to reduce the risk from DDoS attack.
ID	KSP-RE-353
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Preventing injection using white list input validation routines**
Description	Positive or “whitelist” input validation must be used. Such validation should decode any encoded input, and then validate the length, characters, format, type and range on that data before accepting the input. Perform consistency checks at various stages of information being processed.
Supplement	This is not a complete defense as many applications require special characters in their input.
ID	KSP-RE-310
Version	1.1
Date	November 2, 2018
Rationale	Web-based and other application software

Requirement	**HTTP Request Preflight**
Description	Setup a protection against CORS (Cross-Origin Resource Sharing) HTTP request that try to bypass the preflight process.
ID	KSP-RE-354
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Strong authentication and session management controls**
Description	A single set of strong authentication and session management controls must be used. For the requirements see Identity and access management standard and Password security rule.
ID	KSP-RE-311
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software
Rationale	Measures at the end of an employment relationship
Rationale	Authentication
Rationale	Central identity and access management
Rationale	Personal and digital identity
Rationale	Identity and access on the basis of necessity
Rationale	Responsibility for authorizations

Requirement	**Use strong session tokens and protect these**
Description	• Session tokens may not be predictable and able to (reasonably) withstand brute-forcing attacks. • The session ID must simply be an identifier on the client side, and its value must never include sensitive information (or Personal Identifiable Information). The contexts associated to a session ID must be stored on the server side. • Session tokens must not be exposed through other channels. • Session IDs must be have an entropy of at least 112-bit and the value must be derived from a cryptographically secure random number generator. • Session IDs must have a suitable validity period. • Session IDs must be replaced after logging in and deleted with a timeout on the server side. • All existing session tokens/active sessions must expire immediately once credentials have been successfully changed, so that existing sessions on other devices/apps/etc. (based on the old account information) will not remain valid until the normal session expiration time.
ID	KSP-RE-312
Version	1.1
Date	November 2, 2018
Rationale	Web-based and other application software

Requirement	**Indirect Object References per user or session**
Description	Object references should not be predictable and able to withstand brute-forcing attacks. • Per user or session indirect object references must be used. • The application must map the per-user indirect reference back to the actual database key, file or other object on the server.
ID	KSP-RE-313
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Check Access when using Direct Object References**
Description	Each use of a direct object reference from an untrusted source must include an access control check to ensure the user is authorized for the requested object.
ID	KSP-RE-314
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Preventing Cross-Site Request Forgery (CSRF)**
Description	CSRF tokens may not be predictable and must be able to (reasonably) withstand brute-forcing attacks. An unpredictable token must be included in the server response, preferably in a hidden field in the form body. This token must be returned by the client and validated by the server. Such tokens must at a minimum be unique per user session, but can also be unique per request.
ID	KSP-RE-315
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Updating and patching of the (web) application**
Description	All source code, including libraries that are used for generating the (web) application must be maintained and patched for vulnerabilities and stability issues when applicable. Application (code) moving into production must be security tested via code reviews (adhere to OWASP Secure Coding practices) or penetration tests.
ID	KSP-RE-316
Version	1.1
Date	November 2, 2018
Rationale	Web-based and other application software

Requirement	**Application security architecture**
Description	Shared hosting or virtual hosting must not be used without separation on all layers of the application, including the platform on which the application is active, the framework, application specific code and the database.
ID	KSP-RE-317
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Encryption of data at rest**
Description	Encryption of all data at rest is obligatory in cloud resources. For data in KPN data centers it is obligatory to encrypt information classified as Secret. Confidential data is advices to be stored in encrypted form.
Supplement	For cloud resources the following solutions are accepted: AWS KMS AWS CloudHSM Azure Key Vault Hashicorp KeyVault Bring-Your-Own-Key methods are also allowed, assuming they key custodianship with backup policy for the key material is on-par with the solution. It is recommended to ask advice at CISO before using BYOK for business continuity reasons. For other solutions advices is required.
ID	KSP-RE-318
Version	2.0
Date	May 3, 2019
Rationale	Web-based and other application software
Rationale	Information classification
Rationale	Cryptography generic

Requirement	**Strong standard algorithms and keys**
Description	Ensure appropriate strong standard algorithms and strong keys are used to protect sensitive data, and key management is in place.
ID	KSP-RE-320
Version	1.1
Date	April 4, 2018
Rationale	Web-based and other application software
Rationale	Cryptography generic

Requirement	**Proper authentication and authorization for each page**
Description	The enforcement mechanism(s) must deny all access by default, requiring explicit grants to specific users and roles for access to every page.
ID	KSP-RE-321
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Page authorization in a workflow**
Description	If the page is involved in a workflow, it must be verified that conditions are in the proper state to allow access.
ID	KSP-RE-322
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Transport Layer Protection using TLS**
Description	All pages with sensitive data must use TLS. Also, the location to which sensitive data is being posted to must use TLS without redirection from a non-TLS target. Pages containing sensitive data are: - pages displaying sensitive information, e.g. information impacting the privacy of the end-user. - pages which are used for consuming sensitive information, e.g. login forms. Possible exception: when a redirect from the non-TLS location to the TLS location ensures that the end-user is not capable of using the unsecured page.
ID	KSP-RE-323
Version	1.1
Date	April 4, 2018
Rationale	Web-based and other application software
Rationale	Cryptography generic

Requirement	**Transport Layer Protection: sensitive cookies**
Description	The HttpOnly and Secure flag must be set on sensitive cookies.
Supplement	Cookies are often used to store user information, session information and other potentially sensitive information. To prevent sessions hijacking and the leakage of information, these sensitive cookies need to be protected. A more detailed explanation can be found at: https://medium.freecodecamp.org/session-hijacking-and-how-to-stop-it-711e3683d1ac
ID	KSP-RE-324
Version	1.1
Date	May 3, 2019
Rationale	Web-based and other application software
Rationale	Cryptography generic

Requirement	**Transport Layer Protection using strong algorithms only**
Description	Use transport layer security services that are provided by validated cryptomodules. See Cryptography rule and the Cryptographic algorithms and cipher suites tool.
ID	KSP-RE-325
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software
Rationale	Cryptography generic

Requirement	**Transport Layer Protection: certificate validation**
Description	Certificates must be centrally managed, valid, not expired and not revoked. Certificates must also be valid for the domains they serve.
Related info	http://tools.ietf.org/html/rfc5280 http://tools.ietf.org/html/rfc2818 https://tools.ietf.org/html/rfc6125
ID	KSP-RE-326
Version	1.1
Date	April 4, 2018
Rationale	Web-based and other application software
Rationale	Cryptography generic

Requirement	**Transport Layer Protection: backend and other connections**
Description	Backend and other connections must also use TLS or other encryption technologies.
ID	KSP-RE-327
Version	1.1
Date	April 4, 2018
Rationale	Web-based and other application software
Rationale	Cryptography generic

Requirement	**Involvement of user parameters in calculating the destination in redirects and forwards**
Description	Don’t involve user parameters in calculating the destination in redirects and forwards.
ID	KSP-RE-328
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Mapping values as destination parameter**
Description	If destination parameters can’t be avoided, the supplied value must be valid, and authorized for the user. Any such destination parameters must be a mapping value, rather than the actual URL or portion of the URL, and the server side code must translate this mapping to the target URL.
ID	KSP-RE-329
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Reference to responsible disclosure page**
Description	A reference to the responsible disclosure page must be included on the corporate website. This reference should be no more than one click away from the main page. Dutch: https://www.kpn.com/algemeen/missie-en-privacy-statement/beveiligingskwetsbaarheid.htm English: https://www.kpn.com/algemeen/missie-en-privacy-statement/security-vulnerability.htm
ID	KSP-RE-330
Version	1.1
Date	May 3, 2019
Rationale	Web-based and other application software

Requirement	**Maintaining the integrity of information processed**
Description	The integrity of information processed by applications must be maintained by ensuring that: • information is not corrupted when modified by more than one user • information cannot be overwritten accidentally • the processing of information is validated • changes to key ‘static’ information such as customer master files or currency exchange rates are reviewed • unauthorised or incorrect changes to information are detected
ID	KSP-RE-331
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Preventing inaccurate entry of information**
Description	Inaccurate entry of information must be prevented by: • Only accepting data from trusted and authenticated information sources for data changes (creation, change, deletion) • New records have initialization values • Using error messages
ID	KSP-RE-332
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	Output validation
Description	Output validation routines must be used to allow a reader or subsequent processing system to determine if output is within predefined data range and all data is processed.
ID	KSP-RE-333
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	Session Timeout
Description	When a user does not perform any action on a web site during a certain interval (defined by the web server) the status of the user session on the server side must be changed to "not used anymore" and instruct the web server to destroy the user session (deleting all data contained into it). • Set session timeout to the minimal value possible depending on the context of the application. • Avoid "infinite" session timeout. • The session cookie must expire when the browser is closed.
ID	KSP-RE-335
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Brute-Force protection**
Description	Internet facing applications must protect its (user) accounts from brute-force attacks. A process must be in place to detect abusive behavior and a process must be in place to react upon the abuse. Possible origins: • Brute-forcing the password per account. • Brute-forcing the accounts by fixating a password or PIN and brute-forcing this on all accounts. Possible actions: • Detect (rapid) automated login attempts and react by blocking the IP address temporarily. Report to SOC. • After detecting abusive behavior; force the account to logon with a CAPTCHA. Report to SOC. • After detecting abusive behavior; force the account to logon with a second factor. This option assumes there is an opportunity to use SMS or another out of band communication method. Report to SOC.
ID	KSP-RE-337
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Support HTTP Strict Transport Security (HSTS)**
Description	The Strict Transport Security response header must be set to enforce HTTPS. The 'max-age' must be set to at least 5.184.000 seconds (=60 days).
ID	KSP-RE-338
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Mixed Content**
Description	To ensure the proper level of trust with a recipient content must not mix encrypted and unencrypted content. This includes encrypted web pages.
Related info	Mozilla Developer Network: Mixed Content
ID	KSP-RE-339
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**User enumeration**
Description	User enumeration vulnerability must be prevented. User enumeration is not limited to username property of an account. All identifiable property of an account could be used for user enumeration. Possible exception: interfaces purposely developed to list users, accounts or identifiable objects are allowed.
Related info	User Enumeration explained: https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)
ID	KSP-RE-340
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Follow guidelines and best practices**
Description	The development guidelines for security of the underlying platform (e.g. Android, iOS, Windows Phone) must be followed. Platforms offer standard solutions for security, such as for authentication, secure data storage and secure network communications. If best practices exists for security measures that are not explicitly described in the platform's development guidelines, these best practices must be followed.
ID	KSP-RE-341
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	App Permissions
Description	Make the set of permissions that will be required by the mobile app as small as possible. For every permission, describe why it is needed.
ID	KSP-RE-342
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Storage of security related data**
Description	Data that has specific security significance, such as passwords, keys and login tokens, must be stored using the platform's secure storage facilities for security related data. For example: For iOS, use the Keychain For Android, use the KeyStore* For Windows Phone, use the Data Protection API (DPAPI) *For Android devices, which do not feature KeyStore, it is recommended to implement an encrypted container which requires user-input to decrypt. Example: ask for a PIN, use the PIN as input to PBKDF2 and decrypt an AES-encrypted file which holds the credentials.
ID	KSP-RE-343
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Certificate pinning and mutual authentication**
Description	Certificate pinning must not be used and removed where implemented. Apply cyptographic standards for secure data transfer (KSP-RE-410) and implement CAA records (KSP-RE-435). Exception Mobile apps being used as a cryptographic foundation for another eco-system (e.g. key provisioning for another application and context) may implement certificate pinning. When this applies, the pinning method must guarantee business continuity.
Supplement	Applying certificate pinning can have adverse effects on continuity, because app builders: 1. Compromising the endpoint, e.g. mobile device or computer system; 2. Attacking the digitale signature scheme as the foundation to PKI; 3. Compromising a CA, i.e. DigiNotar; 4. Creating a certificate at another CA. The first vector already compromised the endpoint severely. The second requires a mistake in digital signature techniques or a quantum computer with sufficient qubits. The third requires misconduct or infiltration into a CA, whereafter the expectation is that the business for this CA will stop. The fourth vector is mitigated/lowered in risk by applying CAA records on all KPN domains. See KSP-RE-435 for requirements on CAA records.
ID	KSP-RE-344
Version	1.5
Date	August 9, 2019
Rationale	Web-based and other application software

Requirement	**Secure communication downgrade prevention**
Description	The app must prevent that the TLS cipher suite will be downgraded and in this way provides insufficient transport layer protection.
ID	KSP-RE-345
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**User authentication by the backend**
Description	If user specific data will be obtained from the backend server, the app passes the user credentials through to the backend server, all authentication requests must be performed server-side. Upon successful authentication, application data will be loaded onto the mobile device. This will ensure that application data will only be available after successful authentication.
ID	KSP-RE-346
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**User authentication by the app**
Description	If user specific data is obtained from the backend server and/or stored within the app data, the user must be required to authenticate to the app. It is not sufficient to trust only on device authentication.
ID	KSP-RE-347
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	Session management
Description	• Session management must be handled correctly, using appropriate secure protocols, after the initial authentication. For example, require authentication credentials or tokens to be passed with any subsequent request (especially those granting privileged access or modification of data). • Use unpredictable session identifiers. • Invalidate cookies on logout. • Session management should be controlled/managed at server-side. Implementations that rely on stateless sessions, e.g. using JSON Web Tokens (JWT), are not allowed for session management
Related info	The website Pragmatic Web Security offers a great cheatsheet for working with JSON Web Tokes: https://cheatsheets.pragmaticwebsecurity.com/cheatsheets/jwt.pdf
ID	KSP-RE-348
Version	1.3
Date	February 1, 2019
Rationale	Web-based and other application software

Requirement	**Data input from other sources**
Description	Data input through alternative sources directly loaded in the app is forbidden. This should only take place via the explicitly specified backend server.
ID	KSP-RE-349
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Preventing injection using a safe API**
Description	All APIs (in both consumer and producer role) must use a parameterized input methodology to avoid exploitation through an interpreter, e.g. SQL prepare statements or distinct key value pairs. Also, buffer boundaries must be checked explicitly when the environment is susceptible to buffer over- or underflow attacks. If possible, the API must avoid the use of an interpreter.
ID	KSP-RE-306
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Preventing injection using a non-parameterized API**
Description	If a parameterized API is not available, special characters must be carefully escaped using the specific escape syntax for that interpreter.
ID	KSP-RE-307
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Preventing Cross-Site Scripting by escaping all untrusted data**
Description	All untrusted data based on the HTML context (body, attribute, JavaScript, CSS, or URL) must be carefully escaped. This escaping must be included in applications unless the UI framework does this for them.
ID	KSP-RE-309
Version	1.0
Date	December 11, 2017
Rationale	Web-based and other application software

Requirement	**Sensitive data in URL or GET request**
Description	Personally identifiable information, tokens and passwords must not be visible in the URL or parameters of a GET request. Any accompanying credentials must be placed in the header or data fields
ID	KSP-RE-693
Version	1.1
Date	June 18, 2018
Rationale	Web-based and other application software

Requirement	**Referer header**
Description	When an application links to a third party application the leakage of sensitive information should be prevented. For relevant pages the web application must include the appropriate Referrer-Policy in the header.
Supplement	In general applications should prevent the leakage of information. The referer header is one of the sources that could leak information. Example: A web application uses HTTPS and a URL-based session identifier. The web application might wish to link to HTTPS resources on other web sites without leaking the user's session identifier in the URL.
ID	KSP-RE-700
Version	1.0
Date	June 18, 2018
Rationale	Web-based and other application software

Requirement	**Prevent path traversal**
Description	Prevent path traversal, or directory traversal, attacks. Ensure user input is restricted and sanitized and prevent working with user input when using file system calls.
Supplement	Most applications include resources like images, style sheets, scripts, etc. Path traversal attacks, or directory traversal attacks, abuse the unrestricted functionality to load resources by illegally accessing files and directories that are stored outside the web root folder.
Related info	OWASP offers more detailed information on how to prevent path traversal: https://www.owasp.org/index.php/File_System#Path_traversal
ID	KSP-RE-752
Version	1.0
Date	February 1, 2019

Requirement	**Apply Content Security Policy (CSP)**
Description	A web application must define a content security policy (CSP) for each object. The webserver must be configured to deliver the CSP. The Content-Security-Policy HTTP response header field is the preferred mechanism for delivering a policy from a server to a client. As an alternative the CSP can be defined in an element.
Supplement	Content Security Policy (CSP) is an additional layer of security that helps to mitigate the e#ects of a successful content injection, including Cross Site Scripting (XSS) and data injection attacks.
Related info	The Mozilla developers guide offers more detailed information about configuring the Content-Security-Policy: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP Internet Explorer does not support Content-Security-Policy header. It does have limited support when the X-Content-Security-Policy (deprecated) is set. As CSP is an added layer of security it is accepted legacy browsers do not offer this protection.
ID	KSP-RE-751
Version	1.2
Date	November 1, 2019
Rationale	Web-based and other application software

Requirement	**Website, API and portal registration**
Description	Websites, APIs and portals must be registered as asset into the appropriate CMDB.
Supplement	Follow the central ServiceNow process to register websites and portals. APIs are technical assets.
ID	KSP-RE-777
Version	1.0
Date	August 9, 2019
Rationale	Manage Assets
Rationale	Web-based and other application software