Overview of selected KPN Security Policies

Creation date: Wednesday, November 7, 2018 8:06:33 PM

Selected by: Ruud Leurs

Requirement	**Password reset frequency**
Description	Network passwords, e.g. from a KPNNL domain account, and/or second factor tokens may not be reset more than once every 4 hours. In case of an emergency, or if the account needs to be reset sooner, the respective helpdesk must be contacted.
Supplement	To prevent a user from resetting his or her password to the same value, by quickly doing multiple password resets, a timer has been set. However when the helpdesk is not available a user can still regain access to his or her account by waiting.
ID	KSP-RE-250
Version	2.0
Date	August 16, 2018
Rationale	Authentication

Requirement	**One Time Passwords**
Description	An One Time Password (OTP) must only be valid once per context. A context is a combination of a subject (e.g. an account), action (e.g. logon or reset), resource (e.g. particular service interface) and its validity period. An OTP must at least be 6 characters long with a validity period less than 15 minutes.
Supplement	An OTP is a temporary code that can be used as a value for a second factor.
ID	KSP-RE-251
Version	1.1
Date	August 16, 2018
Rationale	Authentication

<table>
<tr><td>Requirement</td><td>Maximum password age</td></tr>
<tr><td>Description</td><td>The password age which a system must support is determined as shown in the table below:

<table>
<tr><th>Account type</th><th>Minimal validity period</th><th>Maximum validity period</th></tr>
<tr><td>Useraccount</td><td>3 months</td><td>6 months*</td></tr>
<tr><td>Administrator/operator account</td><td>3 months</td><td>6 months*</td></tr>
<tr><td>Functional account</td><td>n/a</td><td>24 months</td></tr>
</table>

* The passwords for these accounts are valid for 6 months, when the password storage is using KSP accepted encryption methods or when the account originates from the KPNNL.local domain, maintained by N&I Workspace Services.</td></tr>
<tr><td>ID</td><td>KSP-RE-230</td></tr>
<tr><td>Version</td><td>1.1</td></tr>
<tr><td>Date</td><td>April 4, 2018</td></tr>
<tr><td>Rationale</td><td>Authentication</td></tr>
<tr><td>Rationale</td><td>Measures at the end of an employment relationship</td></tr>
<tr><td>Rationale</td><td>Central identity and access management</td></tr>
<tr><td>Rationale</td><td>Personal and digital identity</td></tr>
<tr><td>Rationale</td><td>Identity and access on the basis of necessity</td></tr>
<tr><td>Rationale</td><td>Responsibility for authorizations</td></tr>
</table>

Requirement	**Hide password on screen**
Description	Passwords must not be visible on the screen in clear text during the login procedure (use obfuscation such as ******** and include confirmation field when defining passwords to avoid errors.
ID	KSP-RE-231
Version	1.0
Date	December 11, 2017
Rationale	Authentication

Requirement	**Account lockout**
Description	Account must be locked for at least 15 minutes after five failed logon attempts. When the failed logon attempts result in a lock-out, the user of the account must be notified about the attempts and informed about the origin of the attempts, e.g. source IP address, country of origin, etc. In addition, the service must have additional measures in place to block the attempts, e.g. blocking the attempts based on source IP-address. If possible the phone number of the security helpdesk must be included in the message to the user.
Supplement	By informing the users that their login accounts are being abused the users can determine if this is them or if an attacker is trying to access their account and a response from the KPN-CERT is required. By adding the number of the security helpdesk the users can quickly respond if the block is not due to their actions.
ID	KSP-RE-232
Version	1.1
Date	August 16, 2018
Rationale	Authentication

Requirement	**Configurable passwords**
Description	Passwords must not be hardcoded in software, but made changeable/ configurable.
ID	KSP-RE-234
Version	1.0
Date	December 11, 2017
Rationale	Authentication

Requirement	**Password transmission**
Description	Before a password is transmitted, the transport channel must be encrypted. When resources need to be transported and viewed all related resources must be transmitted over an encrypted transport channel, e.g. a logon page.
ID	KSP-RE-235
Version	1.0
Date	December 11, 2017
Rationale	Authentication
Rationale	Separating environments
Rationale	Documenting network infrastructure
Rationale	Encrypting network traffic
Rationale	Business Continuity Management (BCM)
Rationale	Designing to availability level

Requirement	**Password storage**
Description	For user accounts: Passwords must be stored irreversible encrypted format (hashed) and salted (to prevent cracking hashed password using “rainbow tables”). For password keeping tools: - The password for the tool should comply with all requirements in this rationale (KSP-RA-227). - Passwords in the tool’s database should be protected with encryption and use message integrity to prevent tampering conform Encryption Algorithms and Hash Algorithms. Passwords may only be reversibly stored when there is an explicit reason to do so. An example use case is KeePass. Also, passwords may be necessary to be able to logon to an adjacent system at the beginning or end of a process. In this particular situation passwords must be stored encrypted and additional measures must be taken to secure the information.
ID	KSP-RE-236
Version	1.0
Date	December 11, 2017
Rationale	Authentication
Rationale	Cryptography generic

Requirement	**Password reset procedure for applications**
Description	In case of a forgotten application password, the password must be reset and sent to the user’s already known (corporate) e-mail address or mobile phone number. An alternative is to send a reset-token or URL with embedded reset-token to guide the user through the reset-functionality process. After receiving a password reset the user must change this password. The replied temporary password or token must have a limited lifetime but must never exceed 24 hours. A good limit is a maximum of 15 minutes validity time. When two factor authentication is part of the account, access to a system must be (re)established using two factor authentication as part of the obligatory password reset. All sessions or session tokens must be reset and a user must re-authenticate before having access to the respective system or application.
Supplement	A strong reset process is required to prevent possible abuse when a users credentials have been compromised for whatever reason.
ID	KSP-RE-237
Version	1.2
Date	November 2, 2018
Rationale	Authentication

Requirement	**Password reset procedure**
Description	When an account requires a password reset by a helpdesk, the helpdesk must identify the user by information not published on the intranet, nor by public information, like a secure question or information exclusively accessible on a national ID card or Company Card. A better solution is to challenge the user by sending an e-mail (when still accessible) or sending an SMS with an OTP. The user can prove his ownership to an account by exchanging the requested information from this message to the helpdesk employee. The user must be informed by sending an e-mail, SMS or both to indicate that the password of the account has been reset and from which means, like a terminal or helpdesk. Communicating passwords in a secure manner can be done over the phone (verbally), via SMS or a password reset link.
Supplement	A strong reset process at the helpdesk is required to prevent possible abuse when a users credentials have been compromised for whatever reason. If user credentials require a second reset within a short timeframe the role of the helpdesk is to prevent an attacker from getting access to the new credentials via social engineering.
ID	KSP-RE-238
Version	1.1
Date	August 16, 2018
Rationale	Authentication

Requirement	**Initial passwords**
Description	Systems must force a user to change an initially provided password (passwords not defined by the user, e.g. passwords provided by the Service Desk) at first usage. The initial password provided to end users does not need to meet the complexity rules, with reservation that it is unique and must be changed at first login into a password that does meet the requirements. If the initial password does meet all password rules then the password needs only to be changed within 2 days after the first use. This includes changing default passwords a system or application comes with before the system or application is put to use. A reset password procedure must never reapply the initial password.
ID	KSP-RE-239
Version	1.2
Date	November 2, 2018
Rationale	Authentication

Requirement	**Distribution of account name and password**
Description	Account names and passwords must be sent in separate electronic or hardcopy messages.
Supplement	When sending a username and password then these may never be combined in the same message irrespective of the medium (e-mail, letter,etc) or manner of it being sent. For example, when sending new account details with a colleague, the username is sent in email A and the password in email B.
ID	KSP-RE-240
Version	1.1
Date	June 18, 2018
Rationale	Authentication

Requirement	**System feedback of failed login**
Description	Systems must respond with a generic message when a logon fails (e.g. “username or password is incorrect”).
ID	KSP-RE-241
Version	1.0
Date	December 11, 2017
Rationale	Authentication

Requirement	**Use of biometrics for authentication on mobile devices (phones, tablets and laptops)**
Description	Biometrics are not allowed as part of a multi factor authentication process, but only as a means to unlock credentials stored in a hardware secure vault solution. E.g. Apple TouchID, Apple FaceID, and fingerprint sensors on Samsung S5 devices or later are acceptable solutions as they all use a secure hardware vault solution to store the fingerprint details. Also Windows Hello is allowed as a biometric solution, assuming the credentials are protected on the device using a TPM 2.0 chip.
Supplement	Biometrics on mobile devices and/or PCs have, at this time, vulnerabilities allowing them to be spoofed by a malicious attacker. Therefore they may never be used as a means of authenticating a user. See KSP-RE-247 for the requirement and list of technically accepted authentication solutions.
ID	KSP-RE-242
Version	1.1
Date	August 16, 2018
Rationale	Authentication

Requirement	**Password history**
Description	Systems must enforce a new password to be different from the last ten passwords.
ID	KSP-RE-243
Version	1.0
Date	December 11, 2017
Rationale	Authentication

Requirement	PIN code
Description	The length of a PIN must be five or more digits. The following PINs are series that must be excluded from use: 12345, 00000, 11111, 22222, 33333, 44444, 55555, 66666, 77777, 88888 and 99999. Using a different amount of digits will result in a similar restriction of use.
ID	KSP-RE-244
Version	1.0
Date	December 11, 2017
Rationale	Authentication

Requirement	**Known origin**
Description	External parties that require remote access to perform IT and TI management for KPN must come from a known origin (IP address), and network filters must be used to enforce this.
ID	KSP-RE-246
Version	1.0
Date	December 11, 2017
Rationale	Authentication

Requirement	**Authentication methods**
Description	Systems must authenticate users based on username and password and, if required, a second factor. The authentication method must comply to the level defined in KSP-GL-713 and the technical and procedural requirements set in KSP-GL-712. The authentication method must be traceable to a natural person unique user and shall not be copied or expire within a short period of time frame (e.g. 5 minutes).
Supplement	Some applications and/or systems have a higher value for KPN and therefore have stricter security requirements. To make sure that the authentication procedure only lets in the correct users certain technical and procedural measures must be in place to support these security requirements. Technically strong authentication methods must be accompanied by an equally strong identity verification procedure in the enrolment of an account.
Related info	
ID	KSP-RE-247
Version	2.0
Date	August 16, 2018
Rationale	Authentication
Rationale	BYOD (Bring Your Own Device)
Rationale	Cryptography generic

Requirement	**Screen-lock and password security**
Description	After 15 minutes of inactivity on the end user device or steppingstone, the user must re-authenticate. If a screensaver is enabled it must always go directly to the lockscreen to re-authenticate the user. Non-interactive workstations with a dedicated purpose of monitoring a system or service on screens are exempt of this policy only when the logged on account can exclusively monitor, but not manipulate nor change anything.
Supplement	Using a timeout prevents a laptop staying unlocked when not in use. If the user triggers a screensaver, for example by using 'Hot Corners' on a MacOS device, then this is a trigger that a user is away from the device therefore requiring the user to re-authenticate when he/she returns.
ID	KSP-RE-248
Version	1.2
Date	August 16, 2018
Rationale	Authentication

Requirement	**User authentication**
Description	End-users must logon to the KPN End User Device using their personal user account and credentials, whereby two-factor authentication is necessary for remote access and signed/encrypted mail.
Supplement	If a KPN user access a KPN device, including Bring-Your-Own devices, then he/she must authenticate with his/her KPN credentials.
ID	KSP-RE-249
Version	1.1
Date	August 16, 2018
Rationale	Authentication

<table>
<tr><td>Requirement</td><td>Password length</td></tr>
<tr><td>Description</td><td>Minimum password length a system must support is determined by the type of account:

<table>
<tr><th>Account Type</th><th>Example</th><th>Min. Length</th></tr>
<tr><td>User account: account without special privileges.</td><td>OTL, KPN werkplek</td><td>10</td></tr>
<tr><td>Admin/operator account: privileged account or has privileges to alter privileges of other accounts.</td><td>Admin/root account, billing account, functional administration</td><td>16</td></tr>
<tr><td>Functional account: accounts used by systems or applications, login and actions are usually automated, accounts are rarely changed.
Also used for pre-shared keys.</td><td>Printer account, VPN with PSK</td><td>24</td></tr>
</table>

For older systems unable to meet these requirements KSP-RE-230 (maximum password age) should be enforced.

Maximum password lengths must not exist. If, for performance reasons, a maximum password length must be imposed, a password of at least 64 characters must be possible.</td></tr>
<tr><td>ID</td><td>KSP-RE-228</td></tr>
<tr><td>Version</td><td>1.2</td></tr>
<tr><td>Date</td><td>November 2, 2018</td></tr>
<tr><td>Rationale</td><td>Authentication</td></tr>
<tr><td>Rationale</td><td>Measures at the end of an employment relationship</td></tr>
<tr><td>Rationale</td><td>Central identity and access management</td></tr>
<tr><td>Rationale</td><td>Personal and digital identity</td></tr>
<tr><td>Rationale</td><td>Identity and access on the basis of necessity</td></tr>
<tr><td>Rationale</td><td>Responsibility for authorizations</td></tr>
<tr><td>Rationale</td><td>Logging</td></tr>
</table>

Requirement	**Password complexity**
Description	Systems must support and enforce passwords containing the full range of printable ASCII characters. Passwords must contain at least three of four groups of characters, which are: at least one uppercase, at least one lowercase, at least one number and at least one other readable character, also known as a special character. This complexity requirement may also be lowered when the system can enforce passwords equal to or longer than 16 characters; guaranteeing that the secure storage of passwords is in accordance with the cryptography requirements for password storage and supports the usage of all printable ASCII characters as input, including the space character.
ID	KSP-RE-229
Version	1.1
Date	August 16, 2018
Rationale	Authentication

Requirement	**Password change responsibility**
Description	For functional (static/system) or shared accounts the account owner is responsible for changing the password in case of a personnel change or change of ownership. Accounts without a password must not result into an interactive logon nor shell. If personnel leave KPN then their password and second factors need to be changed to prevent possible abuse.
Supplement	This requirement is there to prevent abuse of accounts when a KPN'er leaves the company. If one does not remove these accounts it might lead to the person leaving KPN to possibly abuse their previous rights and harm the systems and/ or services of KPN.
ID	KSP-RE-692
Version	1.1
Date	August 16, 2018
Rationale	Authentication
Rationale	Measures at the end of an employment relationship
Rationale	Central identity and access management
Rationale	Personal and digital identity
Rationale	Identity and access on the basis of necessity
Rationale	Responsibility for authorizations
Rationale	Logging

Requirement	**2FA reset procedure**
Description	In case of a forgotten or lost second factor token the provisioning of the token must be restarted as with a new user. All sessions or session tokens must be reset and a user must re-authenticate before having access to the respective system or application.
Supplement	A strong reset process is required to prevent possible abuse when a users credentials have been compromised for whatever reason.
ID	KSP-RE-715
Version	1.0
Date	August 16, 2018
Rationale	Authentication