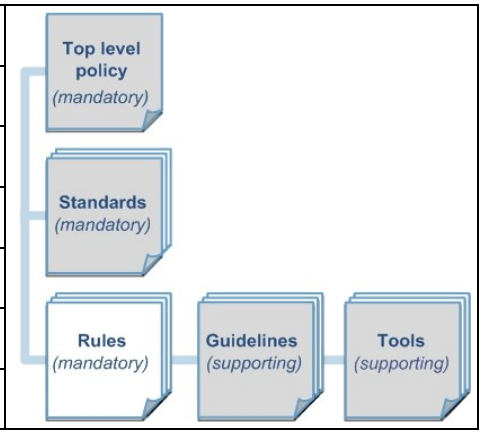
KPN Security Policy

KSP – Rule

Title	**Mobile App Security**
ID	**KSP-FA05-RL13**
Funct. Area	05 - System & Network security
Date	29 July 2016
Version	v1.0
Status	Approved
Owner	CISO



Summary

This policy defines a set of policy rules regarding the protection of mobile applications.
These rules are based primarily on the OWASP Mobile Top 10 2014 and on a release candidate of the OWASP Mobile Top Ten 2016[1].

This policy is written for all KPN NL employees and managers who are involved in developing, maintaining and testing mobile applications. It concerns all mobile applications owned by KPN or mobile applications from vendors/partners that are used for KPN purposes.

Version history

Version	*Date*	*Comments*
v1.0	29 July 2016	First published version

[1] The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted.

ID	KSP-FA05-RL13-R01
Title	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.
Relating document	N/A

ID	KSP-FA05-RL13-R02
Title	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.
Relating document	N/A

ID	KSP-FA05-RL13-R03
Title	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.
Relating document	Requirement: KSP-FA05-RL13-R04 (Storage of application data)

ID	KSP-FA05-RL13-R04
Title	Storage of application data
Description	All application data must be encrypted when stored on the device. This holds for both files and databases. An exception can be made if the data is being exported from the application to the platform's file system when a file must be handled by an external app or on the user's request.
Relating document	KSP-FA05-RL07 - Cryptography

ID	KSP-FA05-RL13-R05
Title	Certificate pinning
Description	To ensure the app connects to the correct backend server, certificate pinning must be applied. The pinning method must guarantee continuity, e.g. to allow for multiple public keys to be pinned.
Relating document	N/A

ID	KSP-FA05-RL13-R06
Title	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.
Relating document	N/A

ID	KSP-FA05-RL13-R07
Title	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.
Relating document	N/A

ID	KSP-FA05-RL13-R08
Title	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.
Relating document	N/A

ID	KSP-FA05-RL13-R09
Title	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).
Relating document	N/A

ID	KSP-FA05-RL13-R10
Title	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.
Relating document	N/A

ID	KSP-FA05-RL13-R11
Title	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.
Relating document	N/A