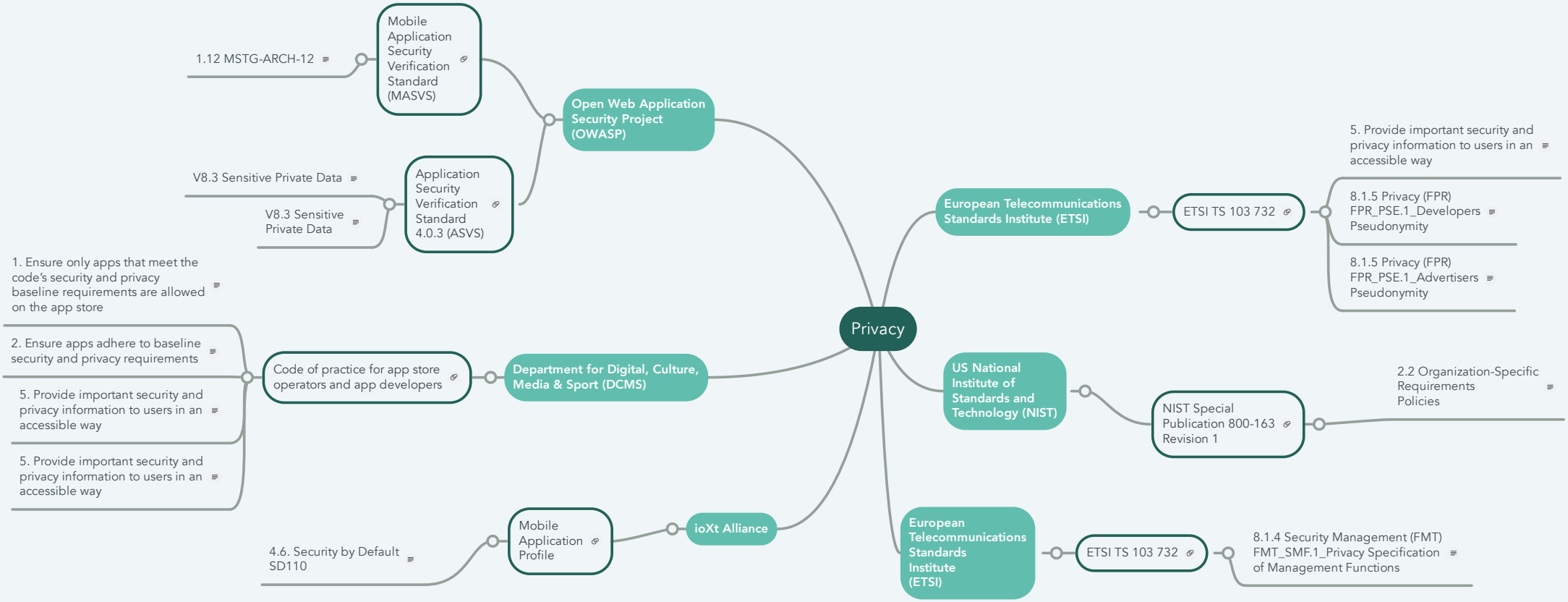
Privacy
Open Web Application Security Project (OWASP)
Mobile Application Security Verification Standard (MASVS)
1.12 MSTG-ARCH-12
Application Security Verification Standard 4.0.3 (ASVS)
V8.3 Sensitive Private Data
V8.3 Sensitive Private Data
Department for Digital, Culture, Media & Sport (DCMS)
Code of practice for app store operators and app developers
1. Ensure only apps that meet the code's security and privacy baseline requirements are allowed on the app store
2. Ensure apps adhere to baseline security and privacy requirements
5. Provide important security and privacy information to users in an accessible way
5. Provide important security and privacy information to users in an accessible way
ioXt Alliance
Mobile Application Profile
4.6. Security by Default SD110
European Telecommunications Standards Institute (ETSI)
ETSI TS 103 732
5. Provide important security and privacy information to users in an accessible way
8.1.5 Privacy (FPR) FPR_PSE.1_Developers Pseudonymity
8.1.5 Privacy (FPR) FPR_PSE.1_Advertisers Pseudonymity
US National Institute of Standards and Technology (NIST)
NIST Special Publication 800-163 Revision 1
2.2 Organization-Specific Requirements Policies
European Telecommunications Standards Institute (ETSI)
ETSI TS 103 732
8.1.4 Security Management (FMT) FMT_SMF.1_Privacy Specification of Management Functions

Privacy

1. European Telecommunications Standards Institute (ETSI)

1.1. ETSI TS 103 732

Link: https://www.etsi.org/deliver/etsi_ts/103700_103799/103732/01.01.01_60/ts_103732v010101p.pdf

1.1.1. 5. Provide important security and privacy information to users in an accessible way

> 5.3 App Store Operators shall display the below information (provided by Developers) for all apps on their app store, such as in a dedicated security and privacy section:
>
> 5.3.1 The jurisdictions where a user's data is stored and processed for each app.[footnote 13]
>
> 5.3.2 The stakeholders that are given access to a user's data. The categories of stakeholders that are displayed to a user should include third party companies, the app's organisation, specific governments or not shared with anyone.
>
> 5.3.3 The purpose of accessing or using a user's data. Categories should include marketing, analytics, user services.
>
> 5.3.4 When the app was last updated and any other relevant security information, as well as the information linked to permissions noted in principle 2.
>
> 5.3.5 The above information shall be written in an accessible format for all users and be clearly available prior to purchase and download.

1.1.2. 8.1.5 Privacy (FPR) FPR_PSE.1_Developers Pseudonymity

> FPR_PSE.1.1/Developers The TSF shall ensure that App developers are unable to determine the Device ID bound to the TSF, unless the App has been permitted access to the Device ID by the human user or this permission was granted by the operating system.
> FPR_PSE.1.2/Developers The TSF shall be able to provide at least one unique alias of the Device ID to each App developer.
> NOTE: Each developer gets a different alias.

1.1.3. 8.1.5 Privacy (FPR) FPR_PSE.1_Advertisers Pseudonymity

> FPR_PSE.1.1/Advertisers The TSF shall ensure that Advertisers in Apps are unable to determine the Device ID bound to the TSF, unless the App has been permitted access to the Device ID by the human user or this permission was
> granted by the operating system. FPR_PSE.1.2/Advertisers The TSF shall be able to provide at least one alias of the Device ID to Advertisers.

2. US National Institute of Standards and Technology (NIST)

2.1. NIST Special Publication 800-163 Revision 1

Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf

2.1.1. 2.2 Organization-Specific Requirements Policies

> The security, privacy and acceptable use policies; social media guidelines; and regulations applicable to the organization.

3. European Telecommunications Standards Institute (ETSI)

3.1. ETSI TS 103 732

Link: https://www.etsi.org/deliver/etsi_ts/103700_103799/103732/01.01.01_60/ts_103732v010101p.pdf

3.1.1. 8.1.4 Security Management (FMT) FMT_SMF.1_Privacy Specification of Management Functions

> FMT_SMF.1.1/Privacy The TSF shall be capable of performing the following management functions by human user:
> • change the alias provided to a particular App developer to a new random alias; and
> • change the alias provided to Advertisers to a new random alias.
> NOTE 3: These aliases are defined in clause 8.1.5.
> NOTE 4: The change of alias can be explicit (for instance by providing a specific option in the app or in the TOE)
> or implicit (for instance rebooting the TOE automatically generates a new alias).

4. ioXt Alliance

4.1. Mobile Application Profile

Link: https://static1.squarespace.com/static/5c6dbac1f8135a29c7fbb621/t/604aa3fa668a8e3b50630433/1615504379349/Mobile_Application_Profile.pdf

4.1.1. 4.6. Security by Default SD110

Provide a privacy policy.

5. Department for Digital, Culture, Media & Sport (DCMS)

5.1. Code of practice for app store operators and app developers

Link: https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers

5.1.1. 1. Ensure only apps that meet the code's security and privacy baseline requirements are allowed on the app store

1.1 App Store Operators shall clearly set out security and privacy requirements for apps on the app store, published in a location that does not require purchasing access by Developers. This shall include those provisions set out in principle 2.

5.1.2. 2. Ensure apps adhere to baseline security and privacy requirements

2.7 Developers should provide users with a mechanism to delete locally held data, and request deletion of personal data gathered by an app.

5.1.3. 5. Provide important security and privacy information to users in an accessible way

5.2 Developers shall provide the following information about an app's behaviour: where a user's data is stored, shared and processed within a privacy policy; when the app was last updated; and other relevant security information.

5.1.4. 5. Provide important security and privacy information to users in an accessible way

> 5.3 App Store Operators shall display the below information (provided by Developers) for all apps on their app store, such as in a dedicated security and privacy section:
>
> 5.3.1 The jurisdictions where a user's data is stored and processed for each app.[footnote 13]
>
> 5.3.2 The stakeholders that are given access to a user's data. The categories of stakeholders that are displayed to a user should include third party companies, the app's organisation, specific governments or not shared with anyone.
>
> 5.3.3 The purpose of accessing or using a user's data. Categories should include marketing, analytics, user services.
>
> 5.3.4 When the app was last updated and any other relevant security information, as well as the information linked to permissions noted in principle 2.
>
> 5.3.5 The above information shall be written in an accessible format for all users and be clearly available prior to purchase and download.

6. Open Web Application Security Project (OWASP)

6.1. Mobile Application Security Verification Standard (MASVS)

Link: https://github.com/OWASP/owasp-masvs/releases/tag/v1.4.2

6.1.1. 1.12 MSTG-ARCH-12

> The app should comply with privacy laws and regulations.

6.2. Application Security Verification Standard 4.0.3 (ASVS)

Link: https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf

6.2.1. V8.3 Sensitive Private Data

> 8.3.2 Verify that users have a method to remove or export their data on demand.

6.2.2. V8.3 Sensitive Private Data

8.3.3 Verify that users are provided clear language regarding collection and use of supplied personal information and that users have provided opt-in consent for the use of that data before it is used in any way.