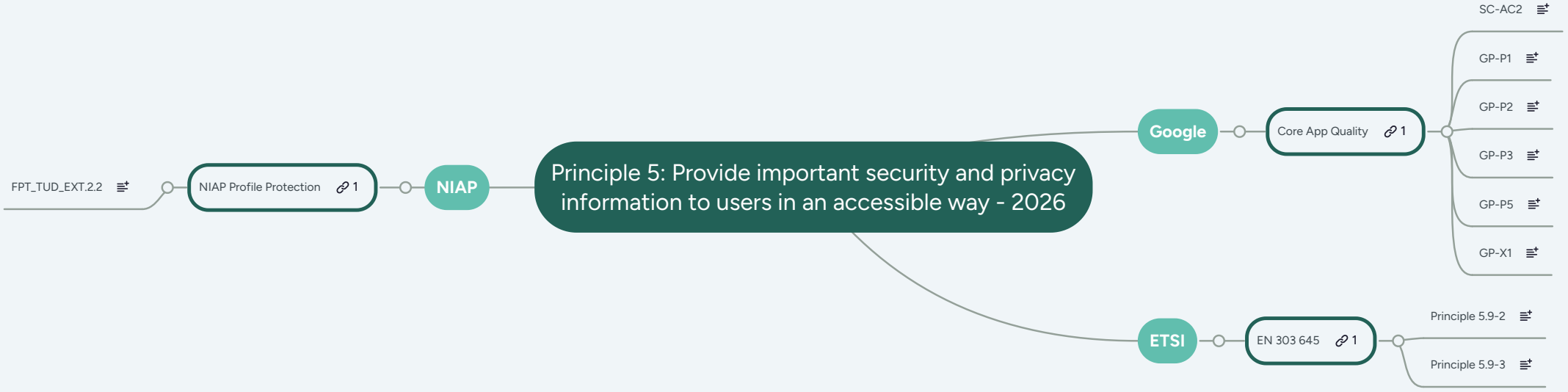
Principle 5: Provide important security and privacy information to users in an accessible way - 2026
NIAP
NIAP Profile Protection 1
FPT_TUD_EXT.2.2
Google
Core App Quality 1
SC-AC2
GP-P1
GP-P2
GP-P3
GP-P5
GP-X1
ETSI
EN 303 645 1
Principle 5.9-2
Principle 5.9-3

Principle 5: Provide important security and privacy information to users in an accessible way - 2026

1. Google

1.1. Core App Quality

Link: https://developer.android.com/docs/quality-guidelines/core-app-quality

Link: https://developer.android.com/docs/quality-guidelines/core-app-quality

1.1.1. SC-AC2

> All intents and broadcasts follow best practices:
>
> Use explicit intents if the destination application is well defined.
> Use Intents to defer permissions to a different app that already has the permission.
> Share data securely across apps.
> Intents that contain a payload are verified before use.
> If you need to pass an Intent to another app, so that the receiving app can invoke and expect a callback in the calling app, do not include a nested intent in the extras. Use a PendingIntent.
> When setting up your PendingIntents, explicitly set the immutable flag, where applicable.

1.1.2. GP-P1

> The app strictly adheres to the terms of the Google Play Developer Content Policy and does not offer inappropriate content, does not use the intellectual property or brand of others, and so on.

1.1.3. GP-P2

> The app maturity level is set appropriately, based on the Content Rating Guidelines.

1.1.4. GP-P3

The app’s feature graphic follows the guidelines outlined in this support article. Make sure that:

The app listing includes a high-quality feature graphic.
The feature graphic does not contain device images, screenshots, or small text that will be illegible when scaled down and displayed on the smallest screen size that your app is targeting.
The feature graphic does not resemble an advertisement.

1.1.5. GP-P5

The app’s screenshots or videos do not represent the content and experience of your app in a misleading way.

1.1.6. GP-X1

Common user-reported bugs in the Reviews tab of the Google Play page are addressed if they are reproducible and occur on many different devices. If a bug occurs on only a few devices, you should still address it if those devices are particularly popular or new.

2. ETSI

2.1. EN 303 645

Link: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

Link: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

2.1.1. Principle 5.9-2

Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.

NOTE: "Recovering cleanly" normally involves resuming connectivity and functionality in the same or improved state.

2.1.2. Principle 5.9-3

The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.

EXAMPLE 1: A Smart Home loses connection to the internet following a power outage. When the network connection is restored, the consumer IoT devices in the home reconnect after a randomized delay to minimize network utilization.

EXAMPLE 2: After making an update available, the manufacturer notifies consumer IoT devices in batches to prevent them all simultaneously downloading the update.

IoT systems and devices are relied upon by consumers for increasingly important use cases that can be safety-relevant or life-impacting. Keeping services running locally if there is a loss of network is one of the measures that can be taken to increase resilience. Other measures can include building redundancy into associated services as well as mitigations against Distributed Denial of Service (DDoS) attacks or signalling storms, which can be caused by mass-reconnections of consumer IoT devices following an outage. It is expected that the level of resilience necessary is proportionate and determined by usage, with consideration given to others that rely on the system, service or consumer IoT device given that an outage can have a wider impact than expected.

Orderly reconnection means in a manner that takes explicit steps to avoid simultaneous requests, such as for software updates or reconnections, from a large number of IoT devices. Such explicit steps can include the introduction of a random delay before a reconnection attempt according to an incremental back-off mechanism.

3. NIAP

3.1. NIAP Profile Protection

Link: https://www.niap-ccevs.org/static_html/protection-profile/516/PP_APP_V2.0.htm

Link: https://www.niap-ccevs.org/static_html/protection-profile/516/PP_APP_V2.0.htm

3.1.1. FPT_TUD_EXT.2.2

The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.