<permission>

SYNTAX:

```
<permission android:description="string resource"
            android:icon="drawable resource"
            android:label="string resource"
            android:name="string"
            android:permissionGroup="string"
            android:protectionLevel=["normal" | "dangerous" |
                                     "signature" | "signatureOrSystem"] />
```

CONTAINED IN:

`<manifest>`

DESCRIPTION:

Declares a security permission that can be used to limit access to specific components or features of this or other applications. See the Permissions section in the introduction, and the Security and Permissions document for more information on how permissions work.

ATTRIBUTES:

`android:description`

A user-readable description of the permission, longer and more informative than the label. It may be displayed to explain the permission to the user — for example, when the user is asked whether to grant the permission to another application.

This attribute must be set as a reference to a string resource; unlike the `label` attribute, it cannot be a raw string.

`android:icon`

A reference to a drawable resource for an icon that represents the permission.

`android:label`

A name for the permission, one that can be displayed to users.

As a convenience, the label can be directly set as a raw string while you're developing the application. However, when the application is ready to be published, it should be set as a reference to a string resource, so that it can be localized like other strings in the user interface.

`android:name`

The name of the permission. This is the name that will be used in code to refer to the permission — for example, in a `<uses-permission>` element and the `permission` attributes of application components.

> **Note:** The system does not allow multiple packages to declare a permission with the same name, unless all the packages are signed with the same certificate. If a package declares a permission, the system does not permit the user to install other packages with the same permission name, unless those packages are signed with the same certificate as the first package. To avoid naming collisions, we recommend using reverse-domain-style naming for custom permissions, for example `com.example.myapp.ENGAGE_HYPERSPACE`.

`android:permissionGroup`

Assigns this permission to a group. The value of this attribute is the name of the group, which must be declared with the `<permission-group>` element in this or another application. If this attribute is not set, the permission does not belong to a group.

`android:protectionLevel`

Characterizes the potential risk implied in the permission and indicates the procedure the system should follow when determining whether or not to grant the permission to an application requesting it. The value can be set to one of the following strings:

Value	Meaning
"`normal`"	The default value. A lower-risk permission that gives requesting applications access to isolated application-level features, with minimal risk to other applications, the system, or the user. The system automatically grants this type of permission to a requesting application at installation, without asking for the user's explicit approval (though the user always has the option to review these permissions before installing).
"`dangerous`"	A higher-risk permission that would give a requesting application access to private user data or control over the device that can negatively impact the user. Because this type of permission introduces potential risk, the system may not automatically grant it to the requesting application. For example, any dangerous permissions requested by an application may be displayed to the user and require confirmation before proceeding, or some other approach may be taken to avoid the user automatically allowing the use of such facilities.
"`signature`"	A permission that the system grants only if the requesting application is signed with the same certificate as the application that declared the permission. If the certificates match, the system automatically grants the permission without notifying the user or asking for the user's explicit approval.
"`signatureOrSystem`"	A permission that the system grants only to applications that are in the Android system image *or* that are signed with the same certificate as the application that declared the permission. Please avoid using this option, as the `signature` protection level should be sufficient for most needs and works regardless of exactly where applications are installed. The "`signatureOrSystem`" permission is used for certain special situations where multiple vendors have applications built into a system image and need to share specific features explicitly because they are being built together.

INTRODUCED IN:

API Level 1

SEE ALSO:

`<uses-permission>`
`<permission-tree>`
`<permission-group>`