



# AppSpecs-Service: Developer-Guidelines for Apps

All too often, TÜV TRUST IT experts find that a lack of knowledge about how to develop secure apps opens unwelcome access gateways. To ensure that your company’s apps, developed in-house or commissioned from third parties, are fully secure and unassailable, TÜV TRUST IT offers assistance in developing secure applications.

## Developer Guidelines for Secure Apps

Using the AppSpecs-Service, essential requirements for secure and trustworthy app-programming can be implemented. To this end, we will provide you with context-specific developer guidelines.

The developer guidelines tool is based on a so-called threat model. Behind it lies a methodical threat analysis that identifies all threats to data protection and data security that an app can cause or to which an application is subject on a smartphone. Generic measures as well as platform-specific implementation guidelines explicated right down to code-level are defined for each and every threat. Beyond this, the types of data processed by the application, statutory provisions and current Best Practices for data handling (e.g. pseudonymous, person-related and sensitive data) are taken into account.

With the help of these guidelines, even developers with little or no experience in the areas of data protection and information security will be able to create secure and unassailable apps.

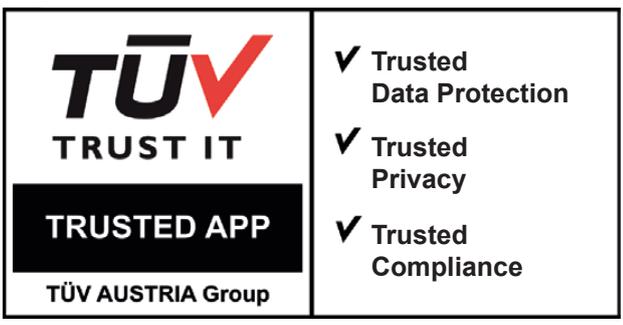
## Customised Implementation Guidelines

Based on the matrix of features defined by the customer/developer, comprising the utilised platform, the type of processed information as well security-relevant aspects, our experts will create an implementation guideline tailored to the particular app. This developer guideline may then function as a security-specific attachment to a specifications sheet. In addition, it allows for a targeted checking of the requirements, pursuant to the development of the app.

## Safety Inspection

As soon as an app is programmed on the basis of the TÜV TRUST IT developer guidelines, the source code can be uploaded to the portal for a TÜV TRUST IT security check. The check concludes with a detailed report that documents and classifies all of the results and the measures proposed. Test reports are sent to the customer in electronic form. The app can then be certified as a “Trusted App”.

Unlike static developer guidelines, the guidelines tool makes a context-based use of security requirements possible so that



Sample Seal “Trusted App”



developers can be provided with guidelines that are related to a specific development project.

**The TÜV TRUST IT AppSpecs-Service supports the following platforms:**

- iOS
- Android

Overview of supported platforms

The function of the guidelines tool consists of drawing up specific implementation guidelines relating to the app in question based on the desired feature matrix defined by the customer or developer, these being the platform used, the kind of data to be processed and the app's security relevant characteristics. The developer guidelines can then serve as a security-specific annex to the specifications. Requirements can also be tested specifically once the app has been developed.

### Your Benefits

- Context-specific guidelines tailored to the individual customer's requirements that are comprehensible even to less experienced developers
- Consideration of security-relevant aspects already during the process of development

**TÜV TRUST IT GmbH**  
TÜV AUSTRIA Group

Waltherstraße 49-51  
D-51069 Köln  
Phone: +49 (0)221 969789 - 0  
Fax: +49 (0)221 969789 -12

**TÜV TRUST IT**  
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1  
A-2345 Brunn am Gebirge  
Phone: +43 (0) 5 0454 - 1000  
Fax: +43 (0) 5 0454 - 76245



[info@tuv-austria.com](mailto:info@tuv-austria.com)  
[www.it-tuv.com](http://www.it-tuv.com)