This master thesis deals with a security analysis for a mobile PKI system. Mobile devices, phones in particular, tend to become the common means as a trusted personal user interface and application platform for mobile and Internet applications. The evolving contactless communication standards (Bluetooth, NFC) shall enable mobile devices to become the GUI for applications that even run outside the device. In order to take advantage of this potential, the communication and transactions should work securely. To achieve this, a PKI is a good start. However, it must be confirmed that running a PKI with mobile devices (phones) does not cut or shorten the usually provided PKI security. Therefore a detailed security analysis is made to identify security threats in the special field of mobile PKI. The results of the security analysis are reported in this master thesis. It is structured in the following way. The introduction gives an overview about PKI in general and the special issues in a mobile PKI environment. It is followed by a description of the involved parties and the target system in section 2. Afterwards the security goals for the target system are stated in section 3. In the next section the security analysis is reported and the identified security threats are stated together with their respective countermeasures, if any. The thesis closes with a conclusion about the discovered results.