X. Questions to Identfy Architectural Security Rules

General Questions

1) Which architecture elements are involved in realizing the building block?
   Examples for architecture elements are components, systems, user etc.
2) Which assumptions are made implicitly (and explicitly of course) and should, therefore, be validated?
3) What state transitions must not happen? What state transitions are allowed explicitly?
   What state transitions are prohibited explicitly? What state transitions are not allowed explicitly? Is there any operation that is implicitly allowed or are all of them prohibited?
4) Are there any default components such as libraries or frameworks that you expect to be used for the implementation? Which weaknesses could be introduced by them?
   Do they for example introduce additional entry points to the system? Which services are offered, which will be used and can services that are not used by the implementation be disabled? How does the default component's interface work? How should it be used? ...

Questions Regarding Authentification and Authorization

5) Which permissions are required to perform each operation?
6) When are validations performed?
   For example authentification, authorization, data etc.

Questions Regarding the Control Flow

7) Which operations are mandatory? When are they performed?
8) What architecture elements may initiate the control flow at which time?
   The elements should be described using a Whitelisting approach
9) Which control flow is prohibited? Which control flow is allowed explicitly?
   What control flow is prohibited explicitly? What control flow is not allowed explicitly? Is there any control flow that is allowed implicitly?

Questions Regarding the Information Flow

10) Which data are sensitive?
    E. g. by law, norm or guideline or because sensitive data is used to calculate new data.
11) Where are trust boundaries within the system?
12) Which sensitive data may cross which trust boundary? Is the crossing subject to a condition?
13) Which data sings are sensitive?
14) Which assumptions are made on data that reach sensitive data sinks and must, therefore, be validated?

Questions on Architectural Relevance

- Does the rule have a local or a non-local impact?
- Does the rule have an intensional or extensional specification?