This Response is Consulted with the following organizations in The Netherlands

netbeheer nederland

Security & Privacy

Security: to protect our vital electricity infrastructure form attacks.

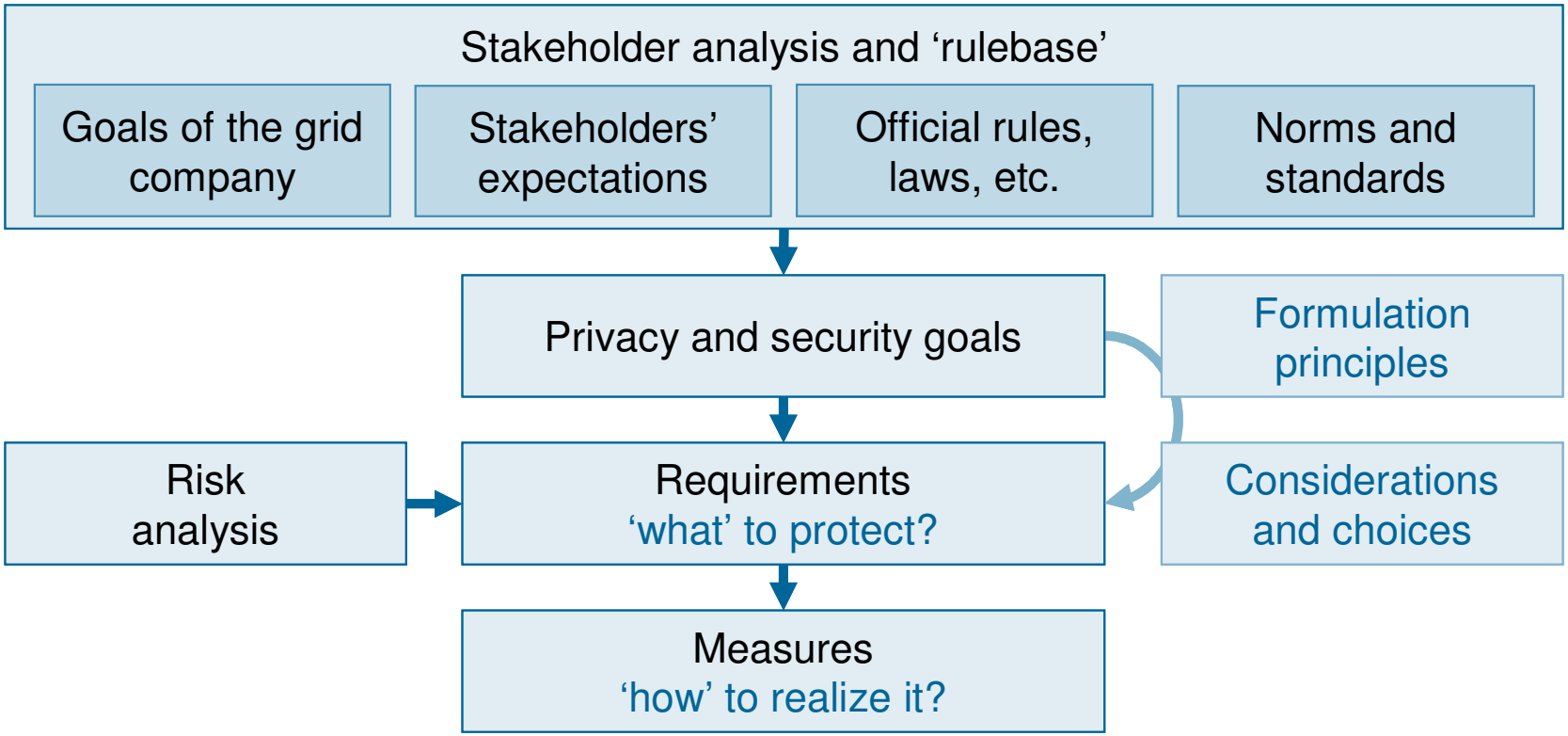
Privacy: to protect our customers' private information.

System security and data protection are crucial issues for the success of the rollout and operation of smart metering and is a vital part of the implementation work in The Netherlands. The Netherlands is taking a rigorous and systematic approach to assessing and managing these issues and developed a data security and privacy regime that both enables smart grid (and smart metering) and protects consumers personal information.

It seems that little security and privacy aspects are being addressed in the ERGEG Draft Guidelines of Good Practice. The Netherlands cannot agree on guidelines that do not sufficiently address security & privacy.

29. Customer control of metering data: Appendix

Dutch Framework Security & Privacy



Additional recommendations

- **Store data locally, except when needed centrally**

  As a basic principle, measurement data can be stored locally (in the smart meter) and is only collected when a customer has provided a mandate for this and when there is a valid reason to collect and use this data. By using this data-pull approach, privacy issues can be addressed, and this will result in a reduction in data communication requirements.

- **Interface with the home (ERGEG Draft Guidelines: table 2/ page 23)**

  The proposed Dutch smart meter configuration is equipped with a local consumer interface (see also page 6 of this document), providing detailed data. This data can be made available to external service providers (and to energy suppliers) by the consumer.

- **Additional functionality can increase complexity**

  System security and data protection are crucial issues for success, but additional requirements for meter functionality can also increase complexity. For example, the Dutch government wants “Customer access to communication data log of meter: insight in exchanged messages and content (in case of metering data). The communication data log is indisputable.”
  This additional functionality will increase the (technical and operational) complexity and cost of smart meter configurations.

- **Strong recommendation**: the discussion in the Netherlands on Smart Meters is focused on three aspects: security/privacy, cost/benefit analysis and future proofness. The cost/benefit analysis conducted in the Netherlands will be translated in English for general use. The security/privacy issues are mentioned on page 4 & 31-34. Future proofness concerns the ability to cost effectively cope with changes in commercial and technical requirements for Smart Metering. The smaller the impact of a change, the larger the future proofness. In the energy market, 2 great unknowns exist: the development of new technologies and how future propositions will look like. The complete system should be able to cope with changes caused by these two items, to make it future proof. Specifications, rules and guidelines should be able to cope with possible future scenarios. European guidelines and national laws state the responsibilities within the energy market. Secondary legislation should state minimal functional requirements on Smart Metering. Technical standards should state the technical characteristics necessary for interoperability between smart metering solutions. Thus, the specifications on the metering interval and number of registers should be specified in the functional and technical standards, which are the documents most easy to change. This creates a future proof European meter.