Appendix 2: Outline of Sophisticated Covert Channel Prevention for Activity `validate`

In order to allow for type validation of a variable containing visibility-restricted information in cases where no risk of information leakage exists, it has to be made sure that throwing the standard `bpel:invalidVariables` fault does not allow conclusions to be drawn as to the value of the information currently contained in this variable. Validation with respect to the proper type of the value contained in a variable may either be caused by a `validate` activity or by indication of attribute `validate="true"` in an `assign` activity. A more sophisticated check for covert channel prevention with type validation than that proposed in the main part of the book would require assuring that no value restricted subtype of a type is being applied in validation.

Therefore, the more sophisticated check for covert channel detection with type validation would allow a variable containing visibility-restricted information to be validated provided its type definition does not imply any restrictions with respect to the value of this variable. This can be checked by inspection of the message type in a WSDL definition or the type definition in an XML schema containing the type definition for the variable under consideration. The XML type definition found for the particular variable must neither contain any `<restriction>` element nor must the type be defined by a `<list>` element nor by a `<union>` element containing any type definition constrained by any of the aforementioned elements.

If the type can be verified in this way to not implying any value range restrictions for the variable under consideration, then type validation may be allowed even in the case where the variable currently contains a value that represents visibility-restricted information.

Klaus-Peter Fischer-Hellmann, *Information Flow Based Security Control Beyond RBAC,* Corporate IT,
DOI 10.1007/978-3-8348-2618-3_11, © Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden 2012