Constructing a Java Card converter using a proof assistant

Thomas Genet, Thomas Jensen and François Monin
Projet Lande, IRISA, Rennes Cedex 35042, France
{genet, jensen, monin}@irisa.fr

The Java Card language is a dialect of Java devoted for the application of smart cards. Due to their limited memory it is important to minimize the size of the code that is to be installed on the card. To do so, once Java Card has been compiled into bytecode, another step is made in order to optimise the latter. Part of this optimisation procedure is given by *tokenisation* from the standard class file format to the CAP file format. The tokenisation procedure consists in replacing names with tokens in an adequate manner to reduce the size of the code.
In this work we are interested in deriving a correct tokenisation algorithm using a proof assistant. To do this, we first formalise a relation between class files and CAP files that defines what is a correct tokenisation. The definition of this relation then guides the proof of correctness of the tokenisation algorithm. To check the feasibility of such a tokenisation and to reduce the complexity, simplification hypotheses have been made regarding packages.
The formal setting has been developed within a framework of a proof checker in order to establish the formal verification and to ensure the correctness of the optimisation.