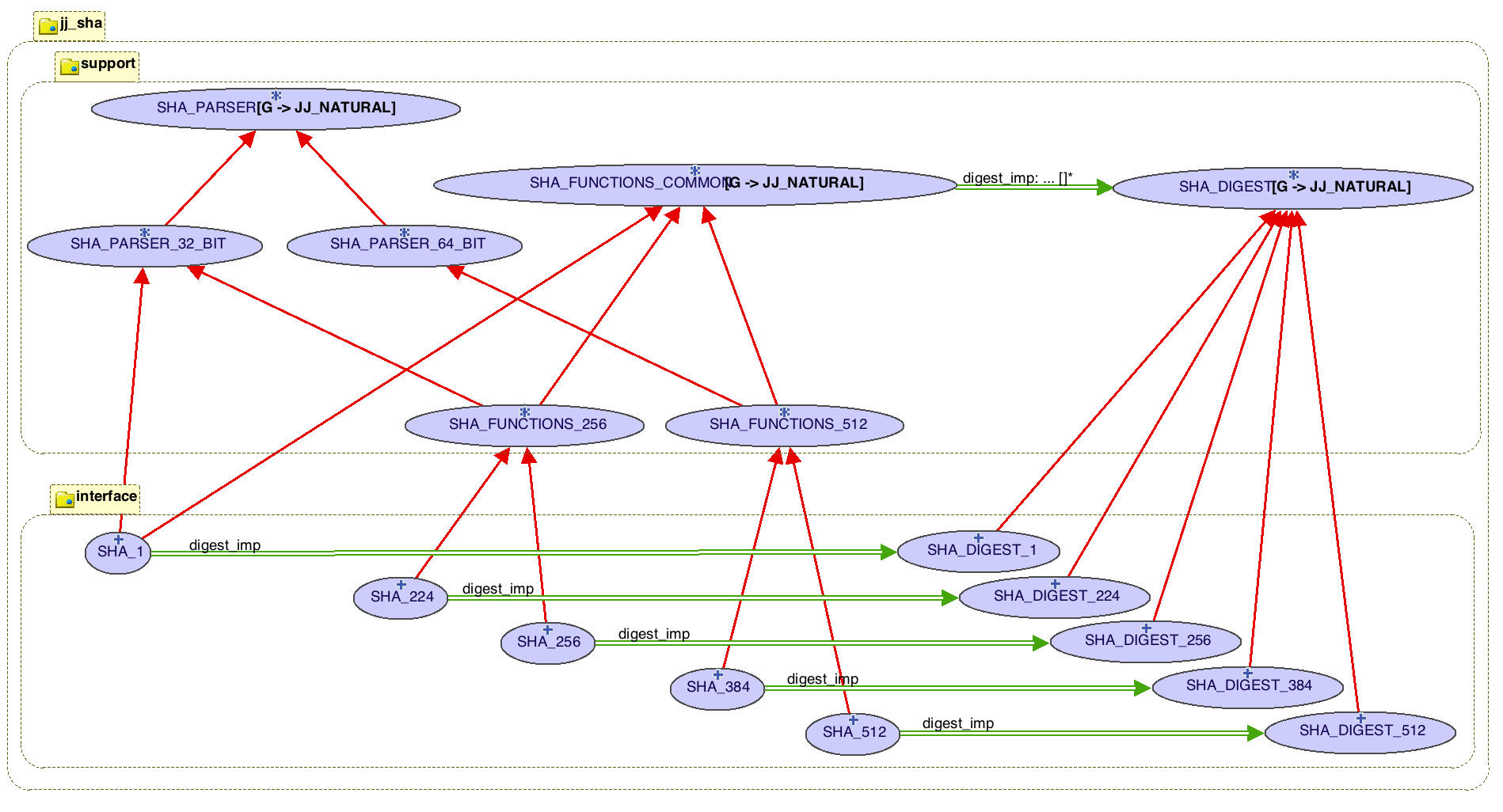
Secure Hash Algorithm Classes



# Interface Cluster

The classes in the interface provide methods for producing a SHA-xxx hash value from a string. An SHA\_xxx object performs the calculations, placing the resulting hash value in a corresponding SHA\_DIGEST\_xxx object.

local

sha\_1: SHA\_1

sha\_512: SHA\_512

d\_1: SHA\_DIGEST\_1

d\_512: SHA\_DIGEST\_512

m: STRING\_8

do

-- Example classes and two ways to use an SHA\_xxx class

m := “abc”

create sha\_1.make (m)

create sha\_512

sha\_512.set\_message (m)

-- Calculate and print the SHA hash tags

d\_1 := sha\_1.digest

d\_512 := sha\_512.digest

print (“SHA-1 value: “ + d\_1.as\_string + “%N”)

print (“SHA-512 value: “ + d\_512.as\_string + “%N”)

end

The output (with some formating) is shown here:

SHA-1 value: a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d

SHA-512 value: ddaf35a193617aba cc417349ae204131 12e6fa4e89a97ea2 0a9eeee64b55d39a

2192992a274fc1a8 36ba3c23a3feebbd 454d4423643ce80e 2a9ac94fa54ca49f

# Support Cluster

The support cluster contains classes that do the work. The SHA\_PARSER and descendents preprocess and pad a message and the SHA\_FUNCTION\_xxx classes perform the hashing. Hash values for the calculations are initialized and maintained in the SHA\_DIGEST\_xxx classes.