CS-Note* 70

Bill J. Ellis
April 14, 2004

Praxis Retreat: Whole System Survey

1 Introduction

Certainly system S contains large segments of pure SPARK. However, system S was developed for SPARKAda 83 and system S is very large. Here focus is placed on the newer and smaller system T, with emphasis on performing a sizable experiment with this code.

2 Labels

2.1 Code classification

- **Variable in type (VIT)**
- **Expressions in base type (EIBT)**
- **For loop range (FLR)**
- **Bring values through code (BVTC)**
- **Bring post and pre conditions through code (BPAPCTC)**
- **Loop recurrence relations (LRR)**
- **Loop termination (LT)**
- **Exploit boolean Assignments (EBA)**
- **Extra cut between if statements (ECBIS)**
- **Extra cut between if statements possible but not used (ECBISPBNU)**
- **Extra cut at no special location (ECANSLU)**
- **Specification information (SI)**
- **Deep algorithm information (DAI)**
- **Propagate non variable property (PNVP)**

2.2 Proof classification

- **Exception freedom (EF) -** Exception freedom proofs.
- **Partial correctness (PC) -** Partial correctness proofs.
- **Refinement integrity (RI) -** Refinement integrity proofs. These prove that the precondition of the abstract state implies the precondition of the refined state and that the postcondition of the refined state implies the postcondition of the abstract state. Essentially proving the refinement integrity VCs shows that the abstraction described is sound.

Note that the following distinctions are made where fairly obvious. Their can be a fine line between these.

- **Hard (H) -** Deeper analysis required!
- **Missing specification rules (MSR) -** Rules missing. These rules are part of the specification - they are very unlikely to be manually discovered.

*Notes in this series are for ϵ-baked ideas, for $1 \geq \epsilon \geq 0$. Only exceptionally should they be cited or distributed outwith the NuSPADE project (EPSRC GR/R24081).

- **Missing Examiner rules (MER) -** Rules missing. These might sensibly be expected to be generated by the Examiner. These are typically for fringe SPARK features. Examples include, generating substitutions for tick delta.
- **Appeal to constant rules (ATCR) -** Proof will involve appealing to replace constant rules. The availability and form of these rules is a problem for both the Examiner and the Simplifier.
- **Tricky non-linear arithmetic (TNLA) -** These are not covered by the proposed changes to the Simplifier. They require some reasoning and dealing with non-linear arithmetic.
- **Stronger specification required (SSR) -** These are not provable with the current specification.

3 System T notes

- Refinement is used.
- Hide is used.
- Named record arguments are everywhere.
- Records are used everywhere.
- Boolean values used.
- Enum values used.
- Constrained subtypes of enum values used.
- Inherit and proper package decomposition is used everywhere.
- Private types are used (type X is new Y with private).
- Private tagged types are used (type X is tagged private).

4 System T

Address: admin.finishop
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -
Notes: - This package employs private types, strings.

Address: admin.init
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: admin.isdoingop
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: admin.ispresent
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: admin.logon
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: admin.logout
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: admin.opisavailable
Code: BVTC + VIT + (DAI: form of constant table)
EF Proof: -
PC Proof: (SSR: constraint on input parameters) + (DAI: reason about constant table?)
RI Proof: -

Address: admin.securityofficerispresent
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: admin.startop
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -
RI Proof: -

Address: admin.thecurrentop
Code: -
EF Proof: -
PC Proof: (MSR: stronger precondition. Not using tightest types?)
RI Proof: -

Address: admintoken.clear
Code: -
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: admintoken.extractuser
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: admintoken.getrole
Code: -
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: admintoken.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: admintoken.iscurrent
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: admintoken.ispresent
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: admintoken.poll
Code: -
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: admintoken.readandcheck
Code: -
EF Proof: -
PC Proof: MSR + SSR
RI Proof: MSR

Address: admintoken.readandcheck.checkauthcert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: admintoken.readandcheck.checkidcertok
Code: -
EF Proof: -
PC Proof: (ATCR: Although it seems the information is present.)
RI Proof: -
Notes: - This package includes operations on strings.

Address: alarm.updatedevice
Code: -
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: auditlog.addelementtofile
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.addelementtolog
Code: -
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: auditlog.addelementtologfile
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.addelementtologfile.addelementtocurrentfile
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.addelementtologfile.addelementtonextfile
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.addelementtologfile.addelementtonextfile.setcurrentfiletonextfreefile
Code: VIT
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.addelementtologfilewithtruncatechecks
Code: BPAPCTC
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: auditlog.archivelog
Code: BVTC + BPAPCTC + VIT + LT
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: auditlog.cancelarchive
Code: VIT
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.checklogalarm
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.clearlogentries
Code: LT + BPAPCTC + PNVP
EF Proof: -
PC Proof: MSR + (DAI: inline subprogram call?!)
RI Proof: MSR

Address: auditlog.deletelogfile
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.getstartandendtimefromfile
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.init
Code: VIT + DAI + SSR + (SI: propagate properties)
EF Proof: -
PC Proof:
RI Proof: -

Address: auditlog.init.setfiledetails
Code: VIT
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.init.setfiledetails.getfiledetails
Code: (VIT: upper bound less one due to immediate increment)
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.nextlistindex
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.systemfaultoccurred
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.theauditalarm
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.truncatelog
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: auditlog.updateendtimefromfile
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: bio.flush
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: bio.getreturncode
Code: VIT + LRR
EF Proof: -
PC Proof: -
RI Proof: -

Address: bio.makedescription
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: bio.poll
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: bio.verify
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert.getdata
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert.getsignature
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert.iscurrent
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert.isok
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: cert.issuerknown
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert.theid
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert.theissuer
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert.themechanism
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr.thebasecert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_auth.clear
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_auth.construct
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_auth.construct.converttistime
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_auth.extract
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_auth.isok
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_auth.setcontents
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_auth.theclearance
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_auth.therole
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_ianda.clear
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_ianda.extract
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_ianda.thetemplate
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_.priv.clear
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_.priv.extract
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_.priv.theclearance
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.attr_.priv.therole
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.id.clear
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.id.extract
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.id.thepublickey
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: cert_.id.thesubject
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: certificatestore.getnextserialnumber
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: certificatestore.getnextserialnumber.stringisoverflowed
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: certificatestore.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: certificatestore.putnextserialnumber
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: certificatestore.serialnumber
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: certificatestore.serialnumberhasoverflowed
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: certificatestore.updatestore
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.addduration
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.constructtime
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.getnow
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.greaterthan
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.greaterthanorequal
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.lessthan
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.lessthanorequal
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.poll
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.printduration
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.printtime
Code: SI
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.setstringsegment
Code: VIT + (DAI: array seen changes - so constrain to this rather than type)
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.splittime
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.startofday
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: clock.thecurrenttime
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: configuration.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: configuration.updatedata
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: display.changedoorunlockedmsg
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: display.combinelines
Code: FLR + BVTC
EF Proof: -
PC Proof: -
RI Proof: -

Address: display.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: display.setvalue
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: display.updatedevice
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: door.failure
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: door.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: door.lockdoor
Code: -
EF Proof: -
PC Proof: SSR
RI Proof: MSR

Address: door.poll
Code: -
EF Proof: -
PC Proof: SSR
RI Proof: MSR

Address: door.thecurrentdoor
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: door.thedooralarm
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: door.unlockdoor
Code: -
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: door.updatedooralarm
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.adminhasdeparted
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.adminlogout
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: MSR

Address: enclave.adminmustlogout
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: enclave.adminop
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.admintokenhasexpired
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.admintokentear
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.archivelogop
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: enclave.archivelogop.finisharchivelog
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.archivelogop.startarchivelog
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.badadmintokentear
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.completefailedadminlogon
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.completefailedenrolment
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.currentadminactivitypossible
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.currentadminactivitypossible.adminactivityinprogress
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.enrolmentisinprogress
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.enrolop
Code: -
EF Proof: SSR
PC Proof: MSR
RI Proof: MSR

Address: enclave.hasshutdown
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.init
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: MSR

Address: enclave.overridedoorlockop
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: enclave.presentadminhasdeparted
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.progressadminactivity
Code: -
EF Proof: SSR
PC Proof: MSR
RI Proof: MSR

Address: enclave.readenrolmentdata
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.resetscreenmessage
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.shutdownop
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: enclave.startadminactivity
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: enclave.startadminactivity.adminlogoncanstart
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.startadminactivity.adminopcanstart
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.startadminactivity.startadminop
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: enclave.updateconfigdataop
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enclave.validateadmintoken
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: MSR

Address: enclave.validateenrolmentdata
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: enrolment.validate
Code: BVTC + (DAI: particular value over quantification in BVTC) + DAI
EF Proof: -
PC Proof: SSR
RI Proof: -

Address: enrolment.validate.validateandaddkey
Code: BVTC + (DAI: particular value over quantification in BVTC)
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: keyboard.finalise
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keyboard.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keyboard.poll
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keyboard.read
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.addkey
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: MSR

Address: keystore.delete
Code: -
EF Proof: -
PC Proof: SSR + MSR
RI Proof: SSR + MSR

Address: keystore.digest
Code: LRR + BVTC + VIT + FLR + (SI: possiblly get as BVTC over procedures)
EF Proof: -
PC Proof: TNLA
RI Proof: -

Address: keystore.digest.getblock
Code: (SI: deep memory constants)
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.dofind
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.issueristhistis
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.isverifiedby
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.keymatchingissuer
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.keymatchingissuerpresent
Code: -
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: keystore.privatekey
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.privatekeypresent
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.sign
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: keystore.thistis
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: latch.failure
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: latch.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: latch.islocked
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: latch.settimeout
Code: -
EF Proof: -
PC Proof: -
RI Proof: MSR

Address: latch.updatedevice
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: MSR

Address: latch.updateinternallatch
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: MSR

Address: poll.activity
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.clearconfigdata
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.clearstats
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.setmessage
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.updatescreen
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.writealarms
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.writeconfigdata
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.writeconfiglabels
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.writecurrenttime
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.writemessage
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.writestatsdata
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: screen.writestatslabels
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: stats.addfailedbio
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: stats.addfailedentry
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: stats.addsuccessfulbio
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: stats.addsuccessfulentry
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: stats.displaystats
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: stats.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tismain
Code: (SI: lots of info at the main loop)
EF Proof: -
PC Proof: -
RI Proof: -

Address: tismain.init
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: tismain.mainloopbody
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: tismain.processing
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: -

Address: tismain.processing.resetscreenmessage
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tismain.shutdownauditlogfailure
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tismain.shutdowndoorlatchfailure
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.getcardstate
Code: -
EF Proof: -
PC Proof: MPR + SSR
RI Proof: -

Address: tokenreader.getcertificate
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.getreaderstate
Code: -
EF Proof: -
PC Proof: MPR + SSR
RI Proof: -

Address: tokenreader.getresponsecode
Code: -
EF Proof: -
PC Proof: MPR + SSR
RI Proof: -

Address: tokenreader.init
Code: - VIT + FLR
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.init.clearreaders
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.init.setreadername
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.makedescription
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.poll
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.poll.checkcardstate
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.poll.checkcardstate.marktokengood
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.poll.disconnecttoken
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.poll.marktokenabsent
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.poll.marktokenbad
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.poll.processreaderstatechange
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: minitokenreader.poll.
processreaderstatechange.marktokenconnected
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.poll.setcurrentstatus
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.poll.setlastfault
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.thetokenid
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.thetokenpresence
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.thetokentry
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: tokenreader.writeauthcertificate
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: updates.activity
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: updates.earlyactivity
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.canstart
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.currentactivitypossible
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.displaypollupdate
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.failedaccesstokenremoved
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.inprogress
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.progress
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: MSR

Address: userentry.readfinger
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.startentry
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.unlockdoor
Code: -
EF Proof: -
PC Proof: MSR
RI Proof: MSR

Address: userentry.updatetoken
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.userhasdeparted
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.usertokentorn
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.validateentry
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.validatefinger
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.validatefinger.achievedfardescription
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: userentry.validateusertoken
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.addauthcert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.clear
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.clearidcert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.extractuser
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.getclass
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.getiandatemplate
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.init
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.ispresent
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.poll
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.readandcheck
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.readandcheck.checkiandacert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.readandcheck.checkidcert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.readandcheck.checkprivcert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.readandcheckauthcert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.readandcheckauthcert.checkauthcert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.readandcheckauthcert.checkidcertok
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

Address: usertoken.updateauthcert
Code: -
EF Proof: -
PC Proof: -
RI Proof: -

5 Impressions

System T contains a fairly small amount of user inserted annotations. In particular, where these annotations are seen they typically only occur for loops and assert type based information. The code is well formed and fairly plain SPARK. There is a fair amount of partial correctness proofs, which the Simplifier typically struggles with as it does not exploit user provided proof rules.