Contents

1 SM0r3Solutions Theory

Built: 16 April 2019
Parent Theories: SM0r3

1.1 Definitions

[certificatesr3a_def]

```
⊢ ∀npriv privcmd cmd.
    certificatesr3a npriv privcmd cmd =
    MAP mkRCert
      (certsr1a npriv privcmd cmd ++
       certsr2root npriv privcmd) ++
    MAP (mkSCert (ca 0)) (certsr2signed npriv privcmd)
```

[certsr1a_def]

```
⊢ ∀npriv privcmd cmd.
    certsr1a npriv privcmd cmd =
    certs npriv privcmd ++
    [reps (Name (Staff Alice)) (Name (Role Commander))
       (prop (SOME cmd));
     reps (Name (Staff Bob)) (Name (Role Operator))
       (prop (SOME cmd))]
```

[certsr2a_def]

```
⊢ ∀npriv privcmd cmd.
    certsr2a npriv privcmd cmd =
    certsr1a npriv privcmd cmd ++ certsr2root npriv privcmd ++
    certsr2signed npriv privcmd
```

1.2 Theorems

[SM0_Commander_privcmd_trapped_lemma]

```
⊢ CFGInterpret (M,Oi,Os)
    (CFG inputOK SM0StateInterp (certs npriv privcmd)
       (Name (Role Commander) says prop (SOME (PR privcmd))::
            ins) s outs) ⇒
  (M,Oi,Os) sat prop NONE
```

[SM0_Commander_trap_privcmd_justified_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (trap (PR privcmd))
      (CFG inputOK SM0StateInterp (certs npriv privcmd)
         (Name (Role Commander) says prop (SOME (PR privcmd))::
              ins) s outs)
      (CFG inputOK SM0StateInterp (certs npriv privcmd) ins
         (NS s (trap (PR privcmd))))
```

```
        (Out s (trap (PR privcmd))::outs)) ⟺
    inputOK
      (Name (Role Commander) says prop (SOME (PR privcmd))) ∧
    CFGInterpret (M,Oi,Os)
      (CFG inputOK SM0StateInterp (certs npriv privcmd)
         (Name (Role Commander) says prop (SOME (PR privcmd))::
              ins) s outs) ∧ (M,Oi,Os) sat prop NONE
```

[SM0r1_Commander_Alice_trap_privcmd_justified_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (trap (PR privcmd))
      (CFG inputOKr1 SM0StateInterp
         (certsr1a npriv privcmd (PR privcmd))
         (Name (Staff Alice) quoting Name (Role Commander) says
          prop (SOME (PR privcmd))::ins) s outs)
      (CFG inputOKr1 SM0StateInterp
         (certsr1a npriv privcmd (PR privcmd)) ins
         (NS s (trap (PR privcmd)))
         (Out s (trap (PR privcmd))::outs)) ⟺
    inputOKr1
      (Name (Staff Alice) quoting Name (Role Commander) says
       prop (SOME (PR privcmd))) ∧
    CFGInterpret (M,Oi,Os)
      (CFG inputOKr1 SM0StateInterp
         (certsr1a npriv privcmd (PR privcmd))
         (Name (Staff Alice) quoting Name (Role Commander) says
          prop (SOME (PR privcmd))::ins) s outs) ∧
    (M,Oi,Os) sat prop NONE
```

[SM0r1_Commander_mapSM0inputOperatorBob_trap_privcmd_justified_thm]

```
⊢ ∀s privcmd outs npriv ins NS Out M Oi Os.
    TR (M,Oi,Os) (trap (PR privcmd))
      (CFG inputOKr1 SM0StateInterp
         (certsr1a npriv privcmd (PR privcmd))
         (mapSM0inputOperatorBob
            (Name (Role Commander) says
             prop (SOME (PR privcmd)))::ins) s outs)
      (CFG inputOKr1 SM0StateInterp
         (certsr1a npriv privcmd (PR privcmd)) ins
         (NS s (trap (PR privcmd)))
         (Out s (trap (PR privcmd))::outs)) ⟺
    inputOKr1
      (mapSM0inputOperatorBob
         (Name (Role Commander) says
          prop (SOME (PR privcmd)))) ∧
    CFGInterpret (M,Oi,Os)
      (CFG inputOKr1 SM0StateInterp
         (certsr1a npriv privcmd (PR privcmd))
         (mapSM0inputOperatorBob
```

```
            (Name (Role Commander) says
             prop (SOME (PR privcmd)))::ins) s outs) ∧
     (M,Oi,Os) sat prop NONE
```

[SM0r1_mapSM0_Alice_Commander_trap_privcmd_lemma]

```
 ⊢ CFGInterpret (M,Oi,Os)
     (CFG inputOKr1 SM0StateInterp
        (certsr1a npriv privcmd (PR privcmd))
        (mapSM0inputOperatorBob
           (Name (Role Commander) says
            prop (SOME (PR privcmd)))::ins) s outs) ⇒
   (M,Oi,Os) sat prop NONE
```

Index