Contents

1 SM0r3Solutions Theory **3**
1.1 Definitions 3
1.2 Theorems 3

1 SM0r3Solutions Theory

Built: 23 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

[certificatesr3a_certsr2a_map_thm]

```
⊢ ∀ npriv privcmd.
    MAP certificateInterpret
      (certificatesr3a npriv privcmd (PR privcmd)) =
    certsr2a npriv privcmd (PR privcmd)
```

[SM0r2_Commander_Alice_trap_privcmd_justified_thm]

```
⊢ ∀ NS Out M Oi Os.
    TR (M,Oi,Os) (trap (PR privcmd))
      (CFG inputOKr2 SM0StateInterp
         (certsr2a npriv privcmd (PR privcmd))
         (Name (KeyS (pubK Alice)) quoting
          Name (Role Commander) says prop (SOME (PR privcmd))::
              ins) s outs)
      (CFG inputOKr2 SM0StateInterp
```

```
          (certsr2a npriv privcmd (PR privcmd)) ins
          (NS s (trap (PR privcmd)))
          (Out s (trap (PR privcmd))::outs)) ⟺
      inputOKr2
        (Name (KeyS (pubK Alice)) quoting
         Name (Role Commander) says prop (SOME (PR privcmd))) ∧
      CFGInterpret (M,Oi,Os)
        (CFG inputOKr2 SM0StateInterp
          (certsr2a npriv privcmd (PR privcmd))
          (Name (KeyS (pubK Alice)) quoting
           Name (Role Commander) says prop (SOME (PR privcmd))::
               ins) s outs) ∧ (M,Oi,Os) sat prop NONE
```

[SM0r2_Commander_mapSM0r1input_trap_privcmd_justifed_thm]

```
 ⊢ ∀NS Out M Oi Os.
      TR (M,Oi,Os) (trap (PR privcmd))
        (CFG inputOKr2 SM0StateInterp
          (certsr2a npriv privcmd (PR privcmd))
          (mapSM0r1input
             (mapSM0inputOperatorBob
                (Name (Role Commander) says
                 prop (SOME (PR privcmd))))::ins) s outs)
        (CFG inputOKr2 SM0StateInterp
          (certsr2a npriv privcmd (PR privcmd)) ins
          (NS s (trap (PR privcmd)))
          (Out s (trap (PR privcmd))::outs)) ⟺
      inputOKr2
        (mapSM0r1input
          (mapSM0inputOperatorBob
             (Name (Role Commander) says
              prop (SOME (PR privcmd))))) ∧
      CFGInterpret (M,Oi,Os)
        (CFG inputOKr2 SM0StateInterp
          (certsr2a npriv privcmd (PR privcmd))
          (mapSM0r1input
             (mapSM0inputOperatorBob
                (Name (Role Commander) says
                 prop (SOME (PR privcmd))))::ins) s outs) ∧
      (M,Oi,Os) sat prop NONE
```

[SM0r2_mapSM0r1_Alice_Commander_trap_privcmd_lemma]

```
 ⊢ CFGInterpret (M,Oi,Os)
      (CFG inputOKr2 SM0StateInterp
         (certsr2a npriv privcmd (PR privcmd))
         (mapSM0r1input
            (mapSM0inputOperatorBob
               (Name (Role Commander) says
                prop (SOME (PR privcmd))))::ins) s outs) ⇒
   (M,Oi,Os) sat prop NONE
```

[SM0r3_Alice_TR2_iff_TR_trap_privcmd]

```
⊢ ∀ NS Out M Oi Os.
    TR2 (M,Oi,Os) (trap (PR privcmd))
      (CFG2 MsgInterpret certificateInterpret inputOKr2
         (certificatesr3a npriv privcmd (PR privcmd))
         SM0StateInterp
         (mkinMsg
            (mapSM0r1input
               (mapSM0inputOperatorBob
                  (Name (Role Commander) says
                   prop (SOME (PR privcmd)))))::ins2) s outs)
      (CFG2 MsgInterpret certificateInterpret inputOKr2
         (certificatesr3a npriv privcmd (PR privcmd))
         SM0StateInterp ins2 (NS s (trap (PR privcmd)))
         (Out s (trap (PR privcmd))::outs)) ⟺
    TR (M,Oi,Os) (trap (PR privcmd))
      (CFG inputOKr2 SM0StateInterp
         (certsr2a npriv privcmd (PR privcmd))
         (Name (KeyS (pubK Alice)) quoting
          Name (Role Commander) says prop (SOME (PR privcmd))::
              ins) s outs)
      (CFG inputOKr2 SM0StateInterp
         (certsr2a npriv privcmd (PR privcmd)) ins
         (NS s (trap (PR privcmd)))
         (Out s (trap (PR privcmd))::outs))
```

[SM0r3_Commander_Alice_privcmd_trap_privcmd_justified_thm]

```
⊢ ∀ NS Out M Oi Os.
    TR2 (M,Oi,Os) (trap (PR privcmd))
      (CFG2 MsgInterpret certificateInterpret inputOKr2
         (certificatesr3a npriv privcmd (PR privcmd))
         SM0StateInterp
         (MSG Alice (Order Commander (PR privcmd))
            (sign (privK Alice)
               (hash (SOME (Order Commander (PR privcmd)))))::
            ins) s outs)
      (CFG2 MsgInterpret certificateInterpret inputOKr2
         (certificatesr3a npriv privcmd (PR privcmd))
         SM0StateInterp ins (NS s (trap (PR privcmd)))
         (Out s (trap (PR privcmd))::outs)) ⟺
    inputOKr2
      (MsgInterpret
         (MSG Alice (Order Commander (PR privcmd))
            (sign (privK Alice)
               (hash
                  (SOME (Order Commander (PR privcmd))))))) ∧
    CFG2Interpret (M,Oi,Os)
      (CFG2 MsgInterpret certificateInterpret inputOKr2
         (certificatesr3a npriv privcmd (PR privcmd))
```

```
          SM0StateInterp
          (MSG Alice (Order Commander (PR privcmd))
             (sign (privK Alice)
                (hash (SOME (Order Commander (PR privcmd))))))::
           ins) s outs) ∧ (M,Oi,Os) sat prop NONE
```

[SM0r3_Commander_Alice_privcmd_trap_privcmd_justified_with_refinements_thm]

```
⊢ ∀NS Out M Oi Os.
    TR2 (M,Oi,Os) (trap (PR privcmd))
      (CFG2 MsgInterpret certificateInterpret inputOKr2
         (certificatesr3a npriv privcmd (PR privcmd))
         SM0StateInterp
         (mkinMsg
            (mapSM0r1input
               (mapSM0inputOperatorBob
                  (Name (Role Commander) says
                   prop (SOME (PR privcmd))))))::ins) s outs)
      (CFG2 MsgInterpret certificateInterpret inputOKr2
         (certificatesr3a npriv privcmd (PR privcmd))
         SM0StateInterp ins (NS s (trap (PR privcmd)))
         (Out s (trap (PR privcmd))::outs)) ⟺
    inputOKr2
      (MsgInterpret
         (mkinMsg
            (mapSM0r1input
               (mapSM0inputOperatorBob
                  (Name (Role Commander) says
                   prop (SOME (PR privcmd)))))))) ∧
    CFG2Interpret (M,Oi,Os)
      (CFG2 MsgInterpret certificateInterpret inputOKr2
         (certificatesr3a npriv privcmd (PR privcmd))
         SM0StateInterp
         (mkinMsg
            (mapSM0r1input
               (mapSM0inputOperatorBob
                  (Name (Role Commander) says
                   prop (SOME (PR privcmd))))))::ins) s outs) ∧
    (M,Oi,Os) sat prop NONE
```

[SM0r3_mkinMsg_SM0r2_Alice_Commander_trap_privcmd_lemma]

```
⊢ CFG2Interpret (M,Oi,Os)
    (CFG2 MsgInterpret certificateInterpret inputOKr2
       (certificatesr3a npriv privcmd (PR privcmd))
       SM0StateInterp
       (mkinMsg
          (mapSM0r1input
             (mapSM0inputOperatorBob
                (Name (Role Commander) says
```

```
                prop (SOME (PR privcmd))))))::ins) s outs) ⇒
(M,Oi,Os) sat prop NONE
```

Index

SM0r3Solutions Theory, 3
Definitions, 3
certificatesr3a_def, 3
certsr1a_def, 3
certsr2a_def, 3
Theorems, 3
certificatesr3a_certsr2a_map_thm, 3
SM0r2_Commander_Alice_trap_privcmd_-justified_thm, 3
SM0r2_Commander_mapSM0r1input_-trap_privcmd_justifed_thm, 4
SM0r2_mapSM0r1_Alice_Commander_-trap_privcmd_lemma, 4
SM0r3_Alice_TR2_iff_TR_trap_privcmd, 5
SM0r3_Commander_Alice_privcmd_trap_-privcmd_justified_thm, 5
SM0r3_Commander_Alice_privcmd_trap_-privcmd_justified_with_refinements_-thm, 6
SM0r3_mkinMsg_SM0r2_Alice_Commander_trap_privcmd_lemma, 6