Contents

1 SM0Solutions Theory

Built: 09 April 2019
Parent Theories: SM0

1.1 Theorems

[Alice_exec_npriv_justified_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (exec (NP npriv))
      (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
         (Name Alice says prop (SOME (NP npriv))::ins) s outs)
      (CFG inputOK SM0StateInterp (certs cmd npriv privcmd) ins
         (NS s (exec (NP npriv)))
         (Out s (exec (NP npriv))::outs)) ⟺
    inputOK (Name Alice says prop (SOME (NP npriv))) ∧
    CFGInterpret (M,Oi,Os)
      (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
         (Name Alice says prop (SOME (NP npriv))::ins) s
         outs) ∧ (M,Oi,Os) sat prop (SOME (NP npriv))
```

[Alice_justified_npriv_exec_thm]

```
⊢ ∀NS Out M Oi Os cmd npriv privcmd ins s outs.
    inputOK (Name Alice says prop (SOME (NP npriv))) ∧
    CFGInterpret (M,Oi,Os)
      (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
         (Name Alice says prop (SOME (NP npriv))::ins) s
         outs) ⇒
    TR (M,Oi,Os) (exec (NP npriv))
      (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
         (Name Alice says prop (SOME (NP npriv))::ins) s outs)
      (CFG inputOK SM0StateInterp (certs cmd npriv privcmd) ins
         (NS s (exec (NP npriv)))
         (Out s (exec (NP npriv))::outs))
```

[Alice_npriv_lemma]

```
⊢ CFGInterpret (M,Oi,Os)
    (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
       (Name Alice says prop (SOME (NP npriv))::ins) s outs) ⇒
  (M,Oi,Os) sat prop (SOME (NP npriv))
```

[Alice_npriv_verified_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (exec (NP npriv))
      (CFG inputOK SM0StateInterp (certs cmd npriv privcmd)
         (Name Alice says prop (SOME (NP npriv))::ins) s outs)
      (CFG inputOK SM0StateInterp (certs cmd npriv privcmd) ins
```

```
        (NS s (exec (NP npriv)))
        (Out s (exec (NP npriv))::outs)) ⇒
    (M,Oi,Os) sat prop (SOME (NP npriv))
```

[Carol_exec_npriv_justified_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (exec (NP npriv))
      (CFG inputOK2 SMOStateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (NP npriv))::ins) s outs)
      (CFG inputOK2 SMOStateInterp (certs2 cmd npriv privcmd)
         ins (NS s (exec (NP npriv)))
         (Out s (exec (NP npriv))::outs)) ⟺
    inputOK2 (Name Carol says prop (SOME (NP npriv))) ∧
    CFGInterpret (M,Oi,Os)
      (CFG inputOK2 SMOStateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (NP npriv))::ins) s
         outs) ∧ (M,Oi,Os) sat prop (SOME (NP npriv))
```

[Carol_justified_npriv_exec_thm]

```
⊢ ∀NS Out M Oi Os cmd npriv privcmd ins s outs.
    inputOK2 (Name Carol says prop (SOME (NP npriv))) ∧
    CFGInterpret (M,Oi,Os)
      (CFG inputOK2 SMOStateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (NP npriv))::ins) s
         outs) ⇒
    TR (M,Oi,Os) (exec (NP npriv))
      (CFG inputOK2 SMOStateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (NP npriv))::ins) s outs)
      (CFG inputOK2 SMOStateInterp (certs2 cmd npriv privcmd)
         ins (NS s (exec (NP npriv)))
         (Out s (exec (NP npriv))::outs))
```

[Carol_justified_privcmd_trap_thm]

```
⊢ ∀NS Out M Oi Os cmd npriv privcmd ins s outs.
    inputOK2 (Name Carol says prop (SOME (PR privcmd))) ∧
    CFGInterpret (M,Oi,Os)
      (CFG inputOK2 SMOStateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (PR privcmd))::ins) s
         outs) ⇒
    TR (M,Oi,Os) (trap (PR privcmd))
      (CFG inputOK2 SMOStateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (PR privcmd))::ins) s
         outs)
      (CFG inputOK2 SMOStateInterp (certs2 cmd npriv privcmd)
         ins (NS s (trap (PR privcmd)))
         (Out s (trap (PR privcmd))::outs))
```

[Carol_npriv_lemma]

```
⊢ CFGInterpret (M,Oi,Os)
    (CFG inputOK2 SM0StateInterp (certs2 cmd npriv privcmd)
       (Name Carol says prop (SOME (NP npriv))::ins) s outs) ⇒
  (M,Oi,Os) sat prop (SOME (NP npriv))
```

[Carol_npriv_verified_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (exec (NP npriv))
      (CFG inputOK2 SM0StateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (NP npriv))::ins) s outs)
      (CFG inputOK2 SM0StateInterp (certs2 cmd npriv privcmd)
         ins (NS s (exec (NP npriv)))
         (Out s (exec (NP npriv))::outs)) ⇒
    (M,Oi,Os) sat prop (SOME (NP npriv))
```

[Carol_privcmd_trap_lemma]

```
⊢ CFGInterpret (M,Oi,Os)
    (CFG inputOK2 SM0StateInterp (certs2 cmd npriv privcmd)
       (Name Carol says prop (SOME (PR privcmd))::ins) s
       outs) ⇒
  (M,Oi,Os) sat prop NONE
```

[Carol_privcmd_trapped_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (trap (PR privcmd))
      (CFG inputOK2 SM0StateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (PR privcmd))::ins) s
         outs)
      (CFG inputOK2 SM0StateInterp (certs2 cmd npriv privcmd)
         ins (NS s (trap (PR privcmd)))
         (Out s (trap (PR privcmd))::outs)) ⇒
    (M,Oi,Os) sat prop NONE
```

[Carol_trap_privcmd_justified_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (trap (PR privcmd))
      (CFG inputOK2 SM0StateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (PR privcmd))::ins) s
         outs)
      (CFG inputOK2 SM0StateInterp (certs2 cmd npriv privcmd)
         ins (NS s (trap (PR privcmd)))
         (Out s (trap (PR privcmd))::outs)) ⟺
    inputOK2 (Name Carol says prop (SOME (PR privcmd))) ∧
    CFGInterpret (M,Oi,Os)
      (CFG inputOK2 SM0StateInterp (certs2 cmd npriv privcmd)
         (Name Carol says prop (SOME (PR privcmd))::ins) s
         outs) ∧ (M,Oi,Os) sat prop NONE
```

Index