

Contents

1	SM0Solutions Theory	3
1.1	Theorems	3

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
```

$$\begin{aligned}
& (NS \ s \ (\text{exec} \ (NP \ npriv))) \\
& (\text{Out} \ s \ (\text{exec} \ (NP \ npriv)) :: \text{outs})) \Rightarrow \\
& (M, Oi, Os) \text{ sat prop } (\text{SOME} \ (NP \ npriv))
\end{aligned}$$

[Carol_exec_npriv_justified_thm]

$$\begin{aligned}
& \vdash \forall NS \ Out \ M \ Oi \ Os. \\
& \quad \text{TR} \ (M, Oi, Os) \ (\text{exec} \ (NP \ npriv)) \\
& \quad (\text{CFG} \ \text{inputOK2} \ \text{SM0StateInterp} \ (\text{certs2} \ \text{cmd} \ npriv \ \text{privcmd}) \\
& \quad \quad (\text{Name} \ \text{Carol} \ \text{says} \ \text{prop} \ (\text{SOME} \ (NP \ npriv)) :: \text{ins}) \ s \ \text{outs}) \\
& \quad (\text{CFG} \ \text{inputOK2} \ \text{SM0StateInterp} \ (\text{certs2} \ \text{cmd} \ npriv \ \text{privcmd}) \\
& \quad \quad \text{ins} \ (NS \ s \ (\text{exec} \ (NP \ npriv)))) \\
& \quad (\text{Out} \ s \ (\text{exec} \ (NP \ npriv)) :: \text{outs})) \iff \\
& \quad \text{inputOK2} \ (\text{Name} \ \text{Carol} \ \text{says} \ \text{prop} \ (\text{SOME} \ (NP \ npriv))) \wedge \\
& \quad \text{CFGInterpret} \ (M, Oi, Os) \\
& \quad (\text{CFG} \ \text{inputOK2} \ \text{SM0StateInterp} \ (\text{certs2} \ \text{cmd} \ npriv \ \text{privcmd}) \\
& \quad \quad (\text{Name} \ \text{Carol} \ \text{says} \ \text{prop} \ (\text{SOME} \ (NP \ npriv)) :: \text{ins}) \ s \\
& \quad \quad \text{outs}) \wedge (M, Oi, Os) \text{ sat prop } (\text{SOME} \ (NP \ npriv))
\end{aligned}$$

[Carol_justified_npriv_exec_thm]

$$\begin{aligned}
& \vdash \forall NS \ Out \ M \ Oi \ Os \ \text{cmd} \ npriv \ \text{privcmd} \ \text{ins} \ s \ \text{outs}. \\
& \quad \text{inputOK2} \ (\text{Name} \ \text{Carol} \ \text{says} \ \text{prop} \ (\text{SOME} \ (NP \ npriv))) \wedge \\
& \quad \text{CFGInterpret} \ (M, Oi, Os) \\
& \quad (\text{CFG} \ \text{inputOK2} \ \text{SM0StateInterp} \ (\text{certs2} \ \text{cmd} \ npriv \ \text{privcmd}) \\
& \quad \quad (\text{Name} \ \text{Carol} \ \text{says} \ \text{prop} \ (\text{SOME} \ (NP \ npriv)) :: \text{ins}) \ s \\
& \quad \quad \text{outs}) \Rightarrow \\
& \quad \text{TR} \ (M, Oi, Os) \ (\text{exec} \ (NP \ npriv)) \\
& \quad (\text{CFG} \ \text{inputOK2} \ \text{SM0StateInterp} \ (\text{certs2} \ \text{cmd} \ npriv \ \text{privcmd}) \\
& \quad \quad (\text{Name} \ \text{Carol} \ \text{says} \ \text{prop} \ (\text{SOME} \ (NP \ npriv)) :: \text{ins}) \ s \ \text{outs}) \\
& \quad (\text{CFG} \ \text{inputOK2} \ \text{SM0StateInterp} \ (\text{certs2} \ \text{cmd} \ npriv \ \text{privcmd}) \\
& \quad \quad \text{ins} \ (NS \ s \ (\text{exec} \ (NP \ npriv)))) \\
& \quad (\text{Out} \ s \ (\text{exec} \ (NP \ npriv)) :: \text{outs}))
\end{aligned}$$

[Carol_justified_privcmd_trap_thm]

$$\begin{aligned}
& \vdash \forall NS \ Out \ M \ Oi \ Os \ \text{cmd} \ npriv \ \text{privcmd} \ \text{ins} \ s \ \text{outs}. \\
& \quad \text{inputOK2} \ (\text{Name} \ \text{Carol} \ \text{says} \ \text{prop} \ (\text{SOME} \ (\text{PR} \ \text{privcmd})))) \wedge \\
& \quad \text{CFGInterpret} \ (M, Oi, Os) \\
& \quad (\text{CFG} \ \text{inputOK2} \ \text{SM0StateInterp} \ (\text{certs2} \ \text{cmd} \ npriv \ \text{privcmd}) \\
& \quad \quad (\text{Name} \ \text{Carol} \ \text{says} \ \text{prop} \ (\text{SOME} \ (\text{PR} \ \text{privcmd})) :: \text{ins}) \ s \\
& \quad \quad \text{outs}) \Rightarrow \\
& \quad \text{TR} \ (M, Oi, Os) \ (\text{trap} \ (\text{PR} \ \text{privcmd})) \\
& \quad (\text{CFG} \ \text{inputOK2} \ \text{SM0StateInterp} \ (\text{certs2} \ \text{cmd} \ npriv \ \text{privcmd}) \\
& \quad \quad (\text{Name} \ \text{Carol} \ \text{says} \ \text{prop} \ (\text{SOME} \ (\text{PR} \ \text{privcmd})) :: \text{ins}) \ s \\
& \quad \quad \text{outs}) \\
& \quad (\text{CFG} \ \text{inputOK2} \ \text{SM0StateInterp} \ (\text{certs2} \ \text{cmd} \ npriv \ \text{privcmd}) \\
& \quad \quad \text{ins} \ (NS \ s \ (\text{trap} \ (\text{PR} \ \text{privcmd})))) \\
& \quad (\text{Out} \ s \ (\text{trap} \ (\text{PR} \ \text{privcmd})) :: \text{outs}))
\end{aligned}$$

[Carol_npriv_lemma]

$\vdash \text{CFGInterpret } (M, Oi, Os)$
 $(\text{CFG inputOK2 SM0StateInterp } (\text{certs2 cmd npriv privcmd})$
 $(\text{Name Carol says prop } (\text{SOME } (\text{NP npriv}))::\text{ins}) s \text{ outs}) \Rightarrow$
 $(M, Oi, Os) \text{ sat prop } (\text{SOME } (\text{NP npriv}))$

[Carol_npriv_verified_thm]

$\vdash \forall NS \text{ Out } M \text{ Oi } Os.$
 $\text{TR } (M, Oi, Os) (\text{exec } (\text{NP npriv}))$
 $(\text{CFG inputOK2 SM0StateInterp } (\text{certs2 cmd npriv privcmd})$
 $(\text{Name Carol says prop } (\text{SOME } (\text{NP npriv}))::\text{ins}) s \text{ outs})$
 $(\text{CFG inputOK2 SM0StateInterp } (\text{certs2 cmd npriv privcmd})$
 $\text{ins } (NS \text{ s } (\text{exec } (\text{NP npriv}))))$
 $(\text{Out } s (\text{exec } (\text{NP npriv}))::\text{outs})) \Rightarrow$
 $(M, Oi, Os) \text{ sat prop } (\text{SOME } (\text{NP npriv}))$

[Carol_privcmd_trap_lemma]

$\vdash \text{CFGInterpret } (M, Oi, Os)$
 $(\text{CFG inputOK2 SM0StateInterp } (\text{certs2 cmd npriv privcmd})$
 $(\text{Name Carol says prop } (\text{SOME } (\text{PR privcmd}))::\text{ins}) s$
 $\text{outs}) \Rightarrow$
 $(M, Oi, Os) \text{ sat prop NONE}$

[Carol_privcmd_trapped_thm]

$\vdash \forall NS \text{ Out } M \text{ Oi } Os.$
 $\text{TR } (M, Oi, Os) (\text{trap } (\text{PR privcmd}))$
 $(\text{CFG inputOK2 SM0StateInterp } (\text{certs2 cmd npriv privcmd})$
 $(\text{Name Carol says prop } (\text{SOME } (\text{PR privcmd}))::\text{ins}) s$
 $\text{outs})$
 $(\text{CFG inputOK2 SM0StateInterp } (\text{certs2 cmd npriv privcmd})$
 $\text{ins } (NS \text{ s } (\text{trap } (\text{PR privcmd}))))$
 $(\text{Out } s (\text{trap } (\text{PR privcmd}))::\text{outs})) \Rightarrow$
 $(M, Oi, Os) \text{ sat prop NONE}$

[Carol_trap_privcmd_justified_thm]

$\vdash \forall NS \text{ Out } M \text{ Oi } Os.$
 $\text{TR } (M, Oi, Os) (\text{trap } (\text{PR privcmd}))$
 $(\text{CFG inputOK2 SM0StateInterp } (\text{certs2 cmd npriv privcmd})$
 $(\text{Name Carol says prop } (\text{SOME } (\text{PR privcmd}))::\text{ins}) s$
 $\text{outs})$
 $(\text{CFG inputOK2 SM0StateInterp } (\text{certs2 cmd npriv privcmd})$
 $\text{ins } (NS \text{ s } (\text{trap } (\text{PR privcmd}))))$
 $(\text{Out } s (\text{trap } (\text{PR privcmd}))::\text{outs})) \iff$
 $\text{inputOK2 } (\text{Name Carol says prop } (\text{SOME } (\text{PR privcmd})))) \wedge$
 $\text{CFGInterpret } (M, Oi, Os)$
 $(\text{CFG inputOK2 SM0StateInterp } (\text{certs2 cmd npriv privcmd})$
 $(\text{Name Carol says prop } (\text{SOME } (\text{PR privcmd}))::\text{ins}) s$
 $\text{outs}) \wedge (M, Oi, Os) \text{ sat prop NONE}$

Index

SM0Solutions Theory, 3

Theorems, 3

Alice_exec_npriv_justified_thm, 3

Alice_justified_npriv_exec_thm, 3

Alice_npriv_lemma, 3

Alice_npriv_verified_thm, 3

Carol_exec_npriv_justified_thm, 4

Carol_justified_npriv_exec_thm, 4

Carol_justified_privcmd_trap_thm, 4

Carol_npriv_lemma, 5

Carol_npriv_verified_thm, 5

Carol_privcmd_trap_lemma, 5

Carol_privcmd_trapped_thm, 5

Carol_trap_privcmd_justified_thm, 5