

## Contents

<b>1 SM0Solutions Theory</b>	<b>3</b>
1.1 Theorems . . . . .	3



# 1 SM0Solutions Theory

**Built:** 09 April 2019

**Parent Theories:** SM0

## 1.1 Theorems

[Alice\_exec\_npriv\_justified\_thm]

$$\vdash \forall NS\ Out\ M\ Oi\ Os.\$$

$$\text{TR} (M, Oi, Os) (\text{exec} (\text{NP } npriv))$$

$$(\text{CFG inputOK SMOStateInterp} (\text{certs } cmd\ npriv\ privcmd)$$

$$(\text{Name Alice says prop (SOME (NP } npriv))::ins\ s\ outs)$$

$$(\text{CFG inputOK SMOStateInterp} (\text{certs } cmd\ npriv\ privcmd) ins$$

$$(NS\ s\ (\text{exec} (\text{NP } npriv)))$$

$$(Out\ s\ (\text{exec} (\text{NP } npriv)))::outs) \iff$$

$$\text{inputOK} (\text{Name Alice says prop (SOME (NP } npriv))) \wedge$$

$$\text{CFGInterpret} (M, Oi, Os)$$

$$(\text{CFG inputOK SMOStateInterp} (\text{certs } cmd\ npriv\ privcmd)$$

$$(\text{Name Alice says prop (SOME (NP } npriv))::ins\ s\ outs) \wedge (M, Oi, Os) \text{ sat prop (SOME (NP } npriv))$$

[Alice\_justified\_npriv\_exec\_thm]

$$\vdash \forall NS\ Out\ M\ Oi\ Os\ cmd\ npriv\ privcmd\ ins\ s\ outs.$$

$$\text{inputOK} (\text{Name Alice says prop (SOME (NP } npriv))) \wedge$$

$$\text{CFGInterpret} (M, Oi, Os)$$

$$(\text{CFG inputOK SMOStateInterp} (\text{certs } cmd\ npriv\ privcmd)$$

$$(\text{Name Alice says prop (SOME (NP } npriv))::ins\ s\ outs) \Rightarrow$$

$$\text{TR} (M, Oi, Os) (\text{exec} (\text{NP } npriv))$$

$$(\text{CFG inputOK SMOStateInterp} (\text{certs } cmd\ npriv\ privcmd)$$

$$(\text{Name Alice says prop (SOME (NP } npriv))::ins\ s\ outs)$$

$$(\text{CFG inputOK SMOStateInterp} (\text{certs } cmd\ npriv\ privcmd) ins$$

$$(NS\ s\ (\text{exec} (\text{NP } npriv)))$$

$$(Out\ s\ (\text{exec} (\text{NP } npriv)))::outs)$$

[Alice\_npriv\_lemma]

$$\vdash \text{CFGInterpret} (M, Oi, Os)$$

$$(\text{CFG inputOK SMOStateInterp} (\text{certs } cmd\ npriv\ privcmd)$$

$$(\text{Name Alice says prop (SOME (NP } npriv))::ins\ s\ outs) \Rightarrow$$

$$(M, Oi, Os) \text{ sat prop (SOME (NP } npriv))$$

[Alice\_npriv\_verified\_thm]

$$\vdash \forall NS\ Out\ M\ Oi\ Os.$$

$$\text{TR} (M, Oi, Os) (\text{exec} (\text{NP } npriv))$$

$$(\text{CFG inputOK SMOStateInterp} (\text{certs } cmd\ npriv\ privcmd)$$

$$(\text{Name Alice says prop (SOME (NP } npriv))::ins\ s\ outs)$$

$$(\text{CFG inputOK SMOStateInterp} (\text{certs } cmd\ npriv\ privcmd) ins$$

---


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

[Carol\_exec\_npriv\_justified\_thm]

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

[Carol\_justified\_npriv\_exec\_thm]

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

[Carol\_justified\_privcmd\_trap\_thm]

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

[Carol\_npriv\_lemma]

```

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

```

[Carol\_npriv\_verified\_thm]

```

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

```

[Carol\_privcmd\_trap\_lemma]

```

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

```

[Carol\_privcmd\_trapped\_thm]

```

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

```

[Carol\_trap\_privcmd\_justified\_thm]

```

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

```



# 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