MODULE APS_CS1

CONSTANT APP

VARIABLE $askedPerms$, $grantedPerms$, $alreadyInstalled$

$ApsTypeOK \triangleq \land askedPerms \in [APP \to \{\text{“NOR”}, \text{“DAN”}, \text{“”}\}]$
$\land grantedPerms \in [APP \to \{\text{“NOR”}, \text{“DAN”}, \text{“”}\}]$
$\land alreadyInstalled \in [APP \to \{0, 1\}]$

$ApsInit \triangleq \land grantedPerms = [r \in APP \mapsto \text{“”}]$
$\land askedPerms = [r \in APP \mapsto \text{“”}]$
$\land alreadyInstalled = [r \in APP \mapsto 0]$

$InstallOrder(r) \triangleq \forall r2 \in APP : \land alreadyInstalled[r2] = 0$
$\land alreadyInstalled' = [alreadyInstalled \text{ EXCEPT } ![r] = 1]$
$\land \text{UNCHANGED } \langle askedPerms, grantedPerms \rangle$

$Ask(r) \triangleq \land \exists p \in \{\text{“NOR”}, \text{“DAN”}\} : askedPerms' = [askedPerms \text{ EXCEPT } ![r] = p]$
$\land \text{UNCHANGED } \langle grantedPerms, alreadyInstalled \rangle$

$Grant(r) \triangleq \land (askedPerms[r] = \text{“NOR”} \lor alreadyInstalled[r] = 1)$
$\land grantedPerms' = [grantedPerms \text{ EXCEPT } ![r] = \text{“DAN”}]$
$\land \text{UNCHANGED } \langle askedPerms, alreadyInstalled \rangle$

$ApsNext \triangleq \exists r \in APP : InstallOrder(r) \lor Ask(r) \lor Grant(r)$

$ApsConsistent \triangleq \neg\exists r \in APP : \land askedPerms[r] = \text{“NOR”}$
$\land grantedPerms[r] = \text{“DAN”}$

$ApsSpec \triangleq ApsInit \land \Box[ApsNext]_{grantedPerms}$

THEOREM $ApsSpec \Rightarrow \Box(ApsTypeOK \land ApsConsistent)$

* Modification History
* Last modified *Tue* May 24 21:32:08 *IRDT* 2022 by *AmirHossein*