APPENDIX

The following Appendices are devoted to the proof of Proposition 1 which establishes that using new session keys at each TMSI reallocation provides unlinkability to MSs. In Appendix A we introduce the necessary definitions and notations. Appendix B provides the proof of Lemma 3 which establishes the bisimulation part of Proposition **??**, while Appendix C details the proof of Lemma 5 which establishes the static part of Proposition 1.

In our quest to understand how proofs of labelled bisimilarity work, and which are the key arguments on which they usually rely, we took the party to detail all the cases even those that look mechanical. This is particularly true for the proof of Lemma 3.

A. DEFINITIONS AND NOTATION

The processes MS and SN model respectively a mobile station and a serving network sharing a private channel dck (the latter models the fact that MS and SN can "securely" establish a shared session key by executing the AKA protocol) are defined as follows:

$$\begin{array}{rcl} MS & \stackrel{def}{=} & \nu\, ck.\nu\, mr.d(x).\overline{up}\langle x\rangle.\overline{dck}\langle ck\rangle.dw(y). \\ & & \quad \mathit{if}\ \ \mathtt{fst}(\mathtt{sdec}(ck,y)) = \text{TMSI\_REALL}\ \ \mathit{then} \\ & & \quad\quad \overline{up}\langle \mathtt{senc}(ck, mr, \text{COMPLETE}))\rangle.\overline{d}\langle \mathtt{snd}(\mathtt{sdec}(ck,y))\rangle \\ & & \quad \mathit{else}\ 0 \\ SN & \stackrel{def}{=} & \nu\, nid.\nu\, sr.dw(\mathrm{z}).dck(xck). \\ & & \quad\quad \overline{up}\langle \mathtt{senc}(xck,\ sr,\ \mathtt{pair}(\text{TMSI\_REALL},\ nid))\rangle.dw(w) \end{array}$$

We also have the following processes, defined earlier:

$$\begin{array}{rcl} Init & \stackrel{def}{=} & \overline{d}\langle id\rangle \\ SSA & \stackrel{def}{=} & \nu\, d.\nu\, id.(Init \mid MS) \\ MSA & \stackrel{def}{=} & \nu\, d.\nu\, id.(Init \mid !MS) \end{array}$$

$Init$ is the memory initialization process, SSA and MSA are respectively a single-session and a multi-session mobile station agent.

Let S and M be two closed processes defined as follows:

$$\begin{array}{rcl} S & \stackrel{def}{=} & \nu\, dck.(!(\nu\, d.\nu\, id.(\overline{d}\langle id\rangle \mid MS) \mid !SN)) \\ & \stackrel{def}{=} & \nu\, dck.(!SSA \mid !SN) \end{array}$$

$$\begin{array}{rcl} M & \stackrel{def}{=} & \nu\, dck.(!(\nu\, d.\nu\, id.(\overline{d}\langle id\rangle \mid !MS) \mid !SN)) \\ & \stackrel{def}{=} & \nu\, dck.(!MSA \mid !SN) \end{array}$$

The process S represents an unbounded number of mobile stations executing the TMSI reallocation procedure at most once. The process M represents an unbounded number of mobile stations which can execute the TMSI reallocation procedure an unbounded number of times.

In the following, the process $MMS^k_{i,j}$ represents the i^{th} mobile station ready to execute the k^{th} step of the j^{th} session of the TMSI reallocation protocol and the process $SMS^k_{i,j}$ represents the $i+j^{th}$ single session mobile station ready to execute the k^{th} step of the TMSI reallocation procedure are. They are defined as in Section 4.3.

We define the grouped multi-session system $GMS_{i,j}[\_]$ representing j sessions of the i^{th} mobile station and the simulating grouped single-session system $GSS_{i,j}[\_]$ representing j single session mobile stations simulating the j sessions of the i^{th} mobile station of the multi-session system, as follows:

$$\begin{array}{rcl} GMS_{i,j}[\_] & \stackrel{def}{=} & \nu\, \widetilde{ms}_{i,j}.\nu\, \widetilde{nid}_{i,l}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,j-1} \mid \_ \mid !RMS_i) \\ GSS_{i,j}[\_] & \stackrel{def}{=} & \nu\, \widetilde{ss}_{i,j}.\nu\, \widetilde{nid}_{i,l}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,j-1} \mid \_) \\ & & l \in \{j-1, j\} \end{array}$$

We define a symmetric relation between the single session and the multiple session system. Let

$$
\begin{aligned}
\mathcal{R} \stackrel{def}{=} \{\ & (C,\ D),\ (D,\ C) : \exists\, n,\ m \geq 0, \\
& A \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PS\,N_m \mid !SSA \mid !SN), \\
& B \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PS\,N_m \mid !MSA \mid !SN), \\
& \text{where } \forall i,\ 1 \leq i \leq n,\ \exists l_i,\ k_{l_i},\ l_i \geq 0, 1 \leq k_{l_i} \leq 8 \\
& \text{such that} \\
& C_i = GSS_{i,l_i}[SMS_{i,l_i}^{k_{l_i}} \mid SSN_{i,l_i}] = \\
& \qquad \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,j}.(SMS_{i,1}^{7} \mid \cdots \mid SMS_{i,l_i-1}^{7} \mid \\
& \qquad SMS_{i,l_i}^{k_{l_i}} \mid SSN_{i,l_i}) \\
& D_i = GMS_{i,l_i}[MMS_{i,l_i}^{k_{l_i}} \mid MSN_{i,l_i}] = \\
& \qquad \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,j}.(MMS_{i,1}^{7} \mid \cdots \mid MMS_{i,l_i-1}^{7} \mid \\
& \qquad MMS_{i,l_i}^{k_{l_i}} \mid MSN_{i,l_i} \mid !RMS_i) \\
& \\
& SSN_{i,l_i} = MSN_{i,l_i} = SN_{i,1}^{h_1} \mid \cdots \mid SN_{i,l_i-1}^{h_{l_i-1}} \mid L^{h_{l_i}}, \\
& h_1, \ldots, h_{l_i-1} \geq 2 \\
& L^{h_{l_i}} = \begin{cases} 0 & \text{if } k_{l_i} \in \{1,\ 2\} \\ SN_{i,l_i}^{h_{l_i}} & \text{otherwise} \end{cases} \\
& \\
& j = \begin{cases} l_i - 1 & \text{if } L^{h_{l_i}} = 0 \\ l_i & \text{otherwise} \end{cases} \\
& \\
& PS\,N_m = SN_{j_1}^{1} \mid \cdots \mid SN_{j_m}^{1}, \\
& \text{for some } j_1, \ldots,\ j_m \in \{0,\ 1\} \\
\} &
\end{aligned}
$$

and let $SSN_{i,0} = MSN_{i,0} = GSS_{i,0}[\_] = GMS_{i,0}[\_] = SMS_{i,0}^{k} = MMS_{i,0}^{k} = 0$. Moreover, we define the set of $\mathcal{S}$ (resp. $\mathcal{M}$) to be the set of single (resp. multi)-session systems:

$$
\begin{aligned}
\mathcal{S} &\stackrel{def}{=} \{C \mid (C, D) \in \mathcal{R} \wedge \\
&\qquad C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PS\,N_m \mid !SSA \mid !SN)\} \\
\mathcal{M} &\stackrel{def}{=} \{D \mid (C, D) \in \mathcal{R} \wedge \\
&\qquad B \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PS\,N_m \mid !MSA \mid !SN)\}
\end{aligned}
$$

B. PROOF OF LEMMA 3

In order to prove Lemma 3 we first establish some auxiliary lemmas. Intuitively, Lemma 1 and Lemma 2 states that if the single (respectively multi)-session system can do a transition then either one of the grouped single (respectively multi)-session system components did the transition (possibly synchronizing with one of the SN_j^1 components of the $PS\,N_m$ process (i.e. the MS synchronizes with the SN network, this steps model the establishment of means for ciphering of the TMSI reallocation protocol) or one of the components under replication was unrolled and did the transition. In particular, Lemma 1 deals with the possible internal transitions of the single (resp. multi)-session system.

LEMMA 1. *Let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PS\,N_m \mid !SA \mid !SN) \in \mathcal{X}$ where either $SA = SSA$ or $SA = MSA$ and either $\mathcal{X} = \mathcal{S}$ or $\mathcal{X} = \mathcal{M}$ accordingly. We have that if $C \xrightarrow{\tau} C'$ then $C' \equiv \nu\, dck.(C_1' \mid \cdots \mid C_{n'}' \mid PS\,N_{m'}' \mid !SA \mid !SN) \in \mathcal{X}$ and*

- *either $\exists i\ C_i \xrightarrow{\tau} C_i' \wedge C_j' = C_j\ \forall j \neq i \wedge n' = n \wedge PS\,N_{m'}' = PS\,N_m$*
- *or $\exists i\ C_i \mid PS\,N_m \xrightarrow{\tau} C_i' \mid PS\,N_{m'}' \wedge C_j' = C_j\ \forall j \neq i \wedge n' = n$*
- *or $n' = n + 1 \wedge C_j' = C'\ \forall j \neq n+1,\ C_{n+1}' = GSS_{n+1,1}[SMS_{n+1,1}^{1} \mid 0]$ if $\mathcal{X} = \mathcal{S}$, $C_{n+1}' = GMS_{n+1,1}[MMS_{n+1,1}^{1} \mid 0]$ if $\mathcal{X} = \mathcal{M}$ and $PS\,N_{m'}' = PS\,N_m$*

PROOF. Let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PS\,N_m \mid !SA \mid !SN) \in \mathcal{X}$ where $SA = SSA$ and $\mathcal{X} = \mathcal{S}$, by definition we have that $C_i \equiv GSS_i[SMS_{i,l_i}^{k_i} \mid SSN_{i,l_i}],\ 1 \leq i \leq n,\ PS\,N_m \equiv SN_{j_1}^{1} \mid \cdots \mid SN_{j_m}^{1}$. If $C \equiv C'' \xrightarrow{\tau} C''' \equiv C'$ then we have that $!SN$ cannot do a silent

transition, while $!SSA$ can do a silent transition (case labelled **New MS**), and $C_i \mid PSN_m$ can do a silent transition on the channel *dck* if $C_i \equiv GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}]$, $k_i = 2$, $m \geq 1$ (case labelled **MS/SN synch**) and C_i can do a silent transition evaluating the conditional statement if $C_i \equiv GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}]$, $k_i = 4$. Hence we have 3 cases:

(i) **(New MS)** $SSA \equiv \nu\, \widetilde{ss}_{n+1,1}.(Init_{n+1,1} \mid SMS^0_{n+1,1}) \xrightarrow{\tau} \nu\, \widetilde{ss}_{n+1,1}.SMS^1_{n+1,1} \equiv \nu\, \widetilde{ss}_{n+1,1}.(SMS^1_{n+1,1} \mid 0) \equiv GSS_{n+1,1}[SMS^1_{n+1,1} \mid 0] = C'_n + 1$ then $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid SSA \mid !SSA \mid !SN) \equiv \nu\, dck.(SSA \mid C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(C'_n + 1 \mid C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid C'_n + 1 \mid PSN_m \mid !SSA \mid !SN) = C'$

(ii) **(MS/SN synch)** Let $1 \leq i \leq n$ such that $C_i \equiv GSS_{i,l_i}[SMS^2_{i,l_i} \mid SSN_{i,l_i}]$ and let $m \geq 1$, we have that $C_i \mid PSN_m \equiv GSS_{i,l_i}[SMS^2_{i,l_i} \mid SSN_{i,l_i}] \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_h} \mid \cdots \mid SN^1_{j_m} \equiv \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,l_i-1} \mid SMS^2_{i,l_i} \mid SSN_{i,l_i-1}) \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_h} \mid \cdots \mid SN^1_{j_m} \equiv \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.\nu\, nid_{j_h}.\nu\, sr_{j_h}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,l_i-1} \mid SMS^2_{i,l_i} \mid SN^1_{j_h} \mid SSN_{i,l_i-1}) \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN_{j_h+1} \mid \cdots \mid SN^1_{j_m} \xrightarrow{\tau} \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.\nu\, nid_{j_h}.\nu\, sr_{j_h}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,l_i-1} \mid SMS^3_{i,l_i} \mid SSN_{i,l_i-1} \mid SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}}\}) \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN_{j_h+1} \mid \cdots \mid SN^1_{j_m} \equiv \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i}.(SMS^{k_1}_{i,1} \mid \cdots \mid SMS^{k_{l_i-1}}_{i,l_i-1} \mid SMS^3_{i,l_i} \mid SSN_{i,l_i-1} \mid SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}}, ^{nid_{i,l_i}}/_{nid_{j_h}}, ^{sr_{i,l_i}}/_{sr_{j_h}}, ^{w_{i,l_i}}/_{w_{j_h}}\}) \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN_{j_h+1} \mid \cdots \mid SN^1_{j_m} \equiv GSS_{i,l_i}[SMS^3_{i,l_i} \mid SSN_{i,l_i}] \mid PSN'_m - 1 = C'_i$, $PSN'_{m-1} = SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN^1_{j_{h+1}} \mid \cdots \mid SN^1_{j_m}$ then $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid PSN_m \mid \cdots \mid C_n \mid !SSA \mid !SN) \equiv \nu\, dck.(C_i \mid PSN_m \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid !SSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(C'_i \mid PSN_{m-1} \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_{m-1} \mid !SSA \mid !SN) = C'$

(iii) Let $1 \leq i \leq n$ such that $C_i \equiv GSS_{i,l_i}[SMS^4_{i,l_i} \mid SSN_{i,l_i}]$ we have 2 cases:

- **(Conditional-then)** if $\texttt{fst}(\texttt{sdec}(ck_{i,l_i}, y_{i,l_i})) =_E$ TMSI_REALL we have that $C_i \xrightarrow{\tau} GSS_{i,l_i}[SMS^5_{i,l_i} \mid SSN_{i,l_i}] = C'_i$, then $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(C'_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) = C'$
- **(Conditional-else)** if $\texttt{fst}(\texttt{sdec}(ck_{i,l_i}, y_{i,l_i})) \neq_E$ TMSI_REALL we have that $C_i \xrightarrow{\tau} GSS_{i,l_i}[SMS^8_{i,l_i} \mid SSN_{i,l_i}] = C'_i$, then $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(C'_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) = C'$

Let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SA \mid !SN) \in \mathcal{X}$ where $SA = MSA$ and $\mathcal{X} = \mathcal{M}$, by definition we have that $C_i \equiv GMS_i[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}]$, $1 \leq i \leq n$, $PSN_m \equiv SN^1_{j_1} \mid \cdots \mid SN^1_{j_m}$. If $C \equiv C'' \xrightarrow{\tau} C''' \equiv C'$ then we have that $!SN$ cannot do a silent transition, while $!MSA$ can do a silent transition (case labelled **New MS**), and $C_i \mid PSN_m$ can do a silent transition on the channel *dck* if $C_i \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}]$, $k_i = 2$, $m \geq 1$ (case labelled **MS/SN synch**), and C_i can do a silent transition either evaluating the conditional statement if $C_i \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}]$, $k_i = 4$ or creating a new session (case labelled **New Session**) if $C_i \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}]$, $k = 6$. Hence we have 4 cases:

(i) **(New MS)** $MSA \equiv \nu\, \widetilde{ms}_{n+1,1}.(Init_{n+1,1} \mid MMS^0_{n+1,1}) \xrightarrow{\tau} \nu\, \widetilde{ms}_{n+1,1}.MMS^1_{n+1,1} \equiv \nu\, \widetilde{ms}_{n+1,1}.(MMS^1_{n+1,1} \mid 0) \equiv GMS_{n+1,1}[MMS^1_{n+1,1} \mid 0] = C'_n + 1$ then $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid MSA \mid !MSA \mid !SN) \equiv \nu\, dck.(MSA \mid C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(C'_n + 1 \mid C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid C'_n + 1 \mid PSN_m \mid !MSA \mid !SN) = C'$

(ii) **(MS/SN synch)** Let $1 \leq i \leq n$ such that $C_i \equiv GMS_{i,l_i}[MMS^2_{i,l_i} \mid MSN_{i,l_i}]$ and let $m \geq 1$, we have that $C_i \mid PSN_m \equiv GMS_{i,l_i}[MMS^2_{i,l_i} \mid MSN_{i,l_i}] \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_h} \mid \cdots \mid SN^1_{j_m} \equiv \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^2_{i,l_i} \mid MSN_{i,l_i-1} \mid !RMS_i) \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_h} \mid \cdots \mid SN^1_{j_m} \equiv \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.\nu\, nid_{j_h}.\nu\, sr_{j_h}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^2_{i,l_i} \mid SN^1_{j_h} \mid MSN_{i,l_i-1} \mid !RMS_i) \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN_{j_h+1} \mid \cdots \mid SN^1_{j_m} \xrightarrow{\tau} \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.\nu\, nid_{j_h}.\nu\, sr_{j_h}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^3_{i,l_i} \mid MSN_{i,l_i-1} \mid SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}}\} \mid !RMS_i) \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN_{j_h+1} \mid \cdots \mid SN^1_{j_m} \equiv \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i}.(MMS^{k_1}_{i,1} \mid \cdots \mid MMS^{k_{l_i-1}}_{i,l_i-1} \mid MMS^3_{i,l_i} \mid MSN_{i,l_i-1} \mid SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}}, ^{nid_{i,l_i}}/_{nid_{j_h}}, ^{sr_{i,l_i}}/_{sr_{j_h}}, ^{w_{i,l_i}}/_{w_{j_h}}\} \mid !RMS_i) \mid SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN_{j_h+1} \mid \cdots \mid SN^1_{j_m} \equiv GMS_{i,l_i}[MMS^3_{i,l_i} \mid MSN_{i,l_i}] \mid PSN'_{m-1} = C'_i$, $PSN'_{m-1} = SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN^1_{j_{h+1}} \mid \cdots \mid SN^1_{j_m}$ then $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid PSN_m \mid \cdots \mid C_n \mid !MSA \mid !SN) \equiv \nu\, dck.(C_i \mid PSN_m \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid !MSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(C'_i \mid PSN_{m-1} \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_{m-1} \mid !MSA \mid !SN) = C'$

(iii) Let $1 \leq i \leq n$ such that $C_i \equiv GMS_{i,l_i}[MMS^4_{i,l_i} \mid MSN_{i,l_i}]$ we have 2 cases:

– **(Conditional-then)** if $\texttt{fst}(\texttt{sdec}(ck_{i,l_i}, y_{i,l_i})) =_E$ TMSI_REALL we have that $C_i \xrightarrow{\tau} GMS_{i,l_i}[MMS^5_{i,l_i} \mid MSN_{i,l_i}] = C'_i$, then $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(C'_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) = C'$

– **(Conditional-else)** if $\texttt{fst}(\texttt{sdec}(ck_{i,l_i}, y_{i,l_i})) \neq_E$ TMSI_REALL we have that $C_i \xrightarrow{\tau} GMS_{i,l_i}[MMS^8_{i,l_i} \mid MSN_{i,l_i}] = C'_i$, then $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(C'_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) = C'$

(ii) **(New session)** let $1 \leq i \leq n,\ k = 6$ then $C_i \equiv GMS_{i,l_i}[SMS^6_{i,l_i} \mid MSN_{i,l_i}] \equiv \nu\, \widetilde{ms}_{i,l_i}.\widetilde{nid}_{i,l_i}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^6_{i,l_i} \mid MSN_{i,l_i} \mid !RMS_i) \equiv \nu\, \widetilde{ms}_{i,l_i}.\widetilde{ms}_{i,l_i}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^6_{i,l_i} \mid MSN_{i,l_i} \mid \nu\, ck_{i,l_i+1} \nu\, mr_{i,l_i+1}.MMS^0_{i,l_i+1} \mid !RMS_i) \xrightarrow{\tau} \nu\, \widetilde{ms}_{i,l_i+1}.\widetilde{nid}_{i,l_i}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^7_{i,l_i} \mid MMS^1_{i,l_i+1} \mid MSN_{i,l_i} \mid !RMS_i) \equiv \nu\, \widetilde{ms}_{i,l_i+1}.\widetilde{nid}_{i,l_i}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i} \mid MMS^1_{i,l_i+1} \mid MSN_{i,l_i} \mid 0 \mid !RMS_i) \equiv GMS_{i,l_i+1}[MMS^1_{i,l_i+1} \mid MSN_{i,l_i+1}] = C'_i$ then $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(C'_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) = C'$

□

Lemma 2 deals with the possible labelled transitions of the single (resp. multi)-session system.

LEMMA 2. *Let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SA \mid !SN) \in \mathcal{X}$ where either $SA = SSA$ or $SA = MSA$ and either $\mathcal{X} = \mathcal{S}$ or $\mathcal{X} = \mathcal{M}$ accordingly. We have that if $C \xrightarrow{\alpha} C'$ with $fv(\alpha) \subseteq dom(C)$ then $C' \equiv \nu\, dck.(C'_1 \mid \cdots \mid C'_{n'} \mid PSN'_{m'} \mid !SA \mid !SN) \in \mathcal{X}$, and*

- *either $\exists i\, C_i \xrightarrow{\alpha} C'_i \wedge C'_j = C_j\ \forall j \neq i \wedge n' = n \wedge PSN'_{m'} = PSN_m$*
- *or $C'_j = C_j\ \forall \wedge n' = n \wedge PSN'_{m'} = PSN_m \mid SN^1_{j_{m+1}},\ m' = m + 1$*

PROOF. Let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SA \mid !SN) \in \mathcal{X}$ where $SA = SSA$ and $\mathcal{X} = \mathcal{S}$, by definition we have that $C_i \equiv GSS_i[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}],\ 1 \leq i \leq n,\ PSN_m \equiv SN^1_{j_1} \mid \cdots \mid SN^1_{j_m}$. If $C \equiv C'' \xrightarrow{\alpha} C''' \equiv C'$ then we have that $!SSA$ and PSN_m cannot do an α-transition, while $!SN$ can do an α-transition (case labelled **SN pre-synch α-transition**), and C_i can do an α-transition if $C_i \equiv GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}],\ k \in \{1, 3, 5\}$ (cases labelled **Active session MS α-transition** and **SN post-synch α-transition**). Hence we have 2 cases:

(i) let $1 \leq i \leq n,\ k \in \{1, 3, 5\}$ then $C_i \equiv GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}]$ we have 2 cases:

– **(Active session MS α-transition)** if $SMS^{k_i}_{i,l_i}$ does the α-transition we have that $C_i \equiv GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}] \xrightarrow{\alpha} GSS_{i,l_i}[SMS^{k_i+1}_{i,l_i} \mid SSN_{i,l_i}] = C'_i$ for all $k \in \{1, 3, 5\}$. Hence $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\alpha} \nu\, dck.(C'_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) = C'$

– **(SN post-synch α-transition)** if SSN_{i,l_i} does the α-transition, let $1 \leq j \leq l_i$ such that $SN^{h_j}_{i,j} \neq 0$ and $2 \leq h_j \leq 3$ we have that $SSN_{i,l_i} \equiv SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_j}_{i,j} \mid \cdots \mid SN^{h_{l_i}}_{i,l_i} \xrightarrow{\alpha} SN^{k_1}_{i,1} \mid \cdots \mid SN^{k_j+1}_{i,j} \mid \cdots \mid SN^{h_{l_i}}_{i,l_i} = SSN'_{i,l_i}$, hence $C_i \equiv GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}] \equiv GSS^{k_i}_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}] \xrightarrow{\alpha} GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN'_{i,l_i}] = C'_i$. Then we have that $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\alpha} \nu\, dck.(C'_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) = C'$

(ii) **(SN pre-synch α-transition)** $!SN \equiv SN^0_h \mid !SN \xrightarrow{\alpha} SN^1_h \mid !SN$ let $PSN_{m+1} = SN^1_{j_1} \mid \cdots \mid SN^1_{j_m} \mid SN^1_h$ then we have that $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !U \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid SN^0_h \mid !SN) \equiv \nu\, dck.(SN^0_h \mid C_i \mid C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\alpha} \nu\, dck.(SN^1_h \mid C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_{m+1} \mid !SSA \mid !SN) = C'$

Let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SA \mid !SN) \in \mathcal{X}$ where $SA = MSA$ and $\mathcal{X} = \mathcal{M}$, by definition we have that $C_i \equiv GMS_i[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}],\ 1 \leq i \leq n,\ PSN_m \equiv SN^1_{j_1} \mid \cdots \mid SN^1_{j_m}$. If $C \equiv C'' \xrightarrow{\alpha} C''' \equiv C'$ then we have that $!MSA$ and PSN_m cannot do an α-transition, while

$!SN$ can do an α-transition (case labelled **SN pre-synch α-transition**), and C_i can do an α-transition if $C_i \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}]$, $k \in \{1,3,5\}$ (cases labelled **Active session MS α-transition** and **SN post-synch α-transition**). Hence we have 2 cases:

(i) let $1 \leq i \leq n$, $k \in \{1,3,5\}$ then $C_i \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}]$ we have 2 cases:

- **(Active session MS α-transition)** if $MMS^{k_i}_{i,l_i}$ does the α-transition we have that $C_i \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}] \xrightarrow{\alpha} GMS_{i,l_i}[MMS^{k_i+1}_{i,l_i} \mid MSN_{i,l_i}] = C'_i$ for all $k \in \{1,3,5\}$. Hence $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\alpha} \nu\, dck.(C'_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) = C'$

- **(SN post-synch α-transition)** if MSN_{i,l_i} does the α-transition, let $1 \leq j \leq l_i$ such that $SN^{h_j}_{i,j} \neq 0$ and $2 \leq h_j \leq 3$ we have that $MSN_{i,l_i} \equiv SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_j}_{i,j} \mid \cdots \mid SN^{h_{l_i}}_{i,l_i} \xrightarrow{\alpha} SN^{k_1}_{i,1} \mid \cdots \mid SN^{k_j+1}_{i,j} \mid \cdots \mid SN^{k_{l_i}}_{i,l_i} = MSN'_{i,l_i}$, hence $C_i \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}] \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}] \xrightarrow{\alpha} GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN'_{i,l_i}] = C'_i$. Then we have that $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\alpha} \nu\, dck.(C'_i \mid C_1 \mid \cdots \mid C_{i-1} \mid C_{i+1} \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C'_i \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) = C'$

(ii) **(SN pre-synch α-transition)** $!SN \equiv SN^0_h \mid !SN \xrightarrow{\alpha} SN^1_h \mid !SN$ let $PSN_{m+1} = SN^1_{j_1} \mid \cdots \mid SN^1_{j_m} \mid SN^1_h$ then we have that $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid SN^0_h \mid !SN) \equiv \nu\, dck.(SN^0_h \mid C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\alpha} \nu\, dck.(SN^1_h \mid C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_{m+1} \mid !MSA \mid !SN) = C'$

□

Intuitively, Lemma 3 states that if one of the components of the single-session system can do a transition then the corresponding component of the multi-session system can do it as well, and vice versa, if a component of the multi-session system can do a transition then the mimicking component of the single-session system can do it as well.

Lemma 3. *Let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SA \mid !SN)$, $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid !\overline{SA} \mid !SN)$ such that $SA = SSA$ (resp. $SA = MSA$) and ($\overline{SA} = MSA$ (resp. $\overline{SA} = SSA$) and $(C, D) \in \mathcal{R}$*
if $C \xrightarrow{\ell} C'$ with $fv(\ell) \subseteq dom(C)$ and $bn(\ell) \cap fn(D) = \emptyset$ then $D \xrightarrow{\ell} D'$ and $(C', D') \in \mathcal{R}$ for any $\ell \in \{\tau, \alpha\}$.

Proof. Let $(C,\ D) \in \mathcal{R}$ and let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid !PSN_m \mid !SSA \mid !SN)$ and $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid !PSN_m \mid !MSA \mid !SN)$.
If $C \xrightarrow{\tau} C'$ then by Lemma 1 we have that $C' \equiv \nu\, dck.(C'_1 \mid \cdots \mid C'_{n'} \mid !PSN'_{m'} \mid !SSA \mid !SN)$ and we have 3 cases:

- $\exists i\ C_i \xrightarrow{\tau} C'_i \wedge C'_j = C_j\ \forall j \neq i \wedge n' = n \wedge PSN'_{m'} = PSN_m$, hence $C_i \equiv GSS_{i,l_i}[SMS^{k_{l_i}}_{i,l_i} \mid SSN_{i,l_i}]$ can do a silent transition this means that C_i is of the form $C_i \equiv GSS_{i,l_i}[SMS^4_{i,l_i} \mid SSN_{i,l_i}]$ i.e. we have two case depending on the evaluation of the conditional statement:

  - **(Conditional-then)** if $C_i \equiv GSS_{i,l_i}[SMS^4_{i,l_i} \mid SSN_{i,l_i}] \xrightarrow{\tau} GSS_{i,l_i}[SMS^5_{i,l_i} \mid SSN_{i,l_i}] = C'_i$ then $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i})) =_E$ TMSI_Reall i.e. $N_{i,l_i} =_E \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_Reall}, z_{i,l_i}))$. By definition of $\mathcal{R}$ we have that $D_i \equiv GMS_{i,l_i}[MMS^4_{i,l_i} \mid MSN_{i,l_i}]$, $MMS^4_{i,l_i} = MX_{i,l_i} \mid MChk_{i,l_i}\{^{N_{i,l_i}}/_{y_{i,l_i}}\}$ and $MChk_{i,l_i}\{^{N_{i,l_i}}/_{y_{i,l_i}}\} \equiv$ *if* $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i})) =$ TMSI_Reall *then* $\overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{Complete})\rangle.\overline{d_{i,1}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i}))\rangle$ *else* $0 \equiv$ *if* $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_Reall}, z_{i,l_i})))) =$ TMSI_Reall *then* $\overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{Complete})\rangle.\overline{d_{i,1}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,l_i}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_Reall}, z_{i,l_i}))))\rangle$ *else* $0 \xrightarrow{\tau} \overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{Complete})\rangle.\overline{d_{i,1}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,j}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_Reall}, z_{i,l_i}))))\rangle$ hence $MMS^4_{i,l_i} \xrightarrow{\tau} MMS^5_{i,l_i}$ and $D_i \xrightarrow{\tau} GMS_{i,l_i}[MMS^5_{i,l_i} \mid MSN_{i,l_i}] = D'_i$ then let $D' = \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN)$ we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(D_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(D'_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) = D'$ and $(C',\ D') \in \mathcal{R}$
  - **(Conditional-else)** if $C_i \equiv GSS_{i,l_i}[SMS^4_{i,l_i} \mid SSN_{i,l_i}] \xrightarrow{\tau} GSS_{i,l_i}[SMS^8_{i,l_i} \mid SSN_{i,l_i}] = C'_i$ then $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i})) \neq_E$ TMSI_Reall i.e. $N_{i,l_i} \neq_E \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_Reall}, z_{i,l_i}))$. By definition of $\mathcal{R}$ we have that $D_i \equiv GMS_{i,l_i}[MMS^4_{i,l_i} \mid MSN_{i,l_i}]$, $MMS^4_{i,l_i} = MX_{i,l_i} \mid MChk_{i,l_i}\{^{N_{i,l_i}}/_{y_{i,l_i}}\}$ and $MChk_{i,l_i}\{^{N_{i,l_i}}/_{y_{i,l_i}}\} \equiv$ *if* $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i})) =$ TMSI_Reall *then* $\overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{Complete})\rangle.\overline{d_{i,1}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i}))\rangle$ *else* $0 \equiv$ *if* $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_Reall}, z_{i,l_i}))) =$

TMSI_REALL *then* $\overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{COMPLETE})\rangle.\ \overline{d_{i,1}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,l_i}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_REALL}, z_{i,l_i})))\rangle$ *else* $0 \xrightarrow{\tau} 0$ hence $MMS^4_{i,l_i} \xrightarrow{\tau} MMS^8_{i,l_i}$ and $D_i \xrightarrow{\tau} GMS_{i,l_i}[MMS^8_{i,l_i} \mid MSN_{i,l_i}] = D'_i$ then let $D' = \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA\ !SN)$ we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_i \mid \cdots \mid D_n \mid PSN_m\ !MSA\ !SN) \equiv \nu\, dck.(D_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m\ !MSA\ !SN) \xrightarrow{\tau} \nu\, dck.(D'_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !MSA\ !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA\ !SN) = D'$ and $(C',\ D') \in \mathcal{R}$

- **(MS/SN synch)** $\exists i\ C_i \mid PSN_m \xrightarrow{\tau} C'_i \mid PSN'_{m'} \wedge C'_j = C_j\ \forall j \neq i \wedge n' = n$ the only possible silent transition between C_i and PSN_m is the communication on the channel dck hence, $C_i \equiv GSS_{i,l_i}[SMS^2_{i,l_i} \mid SSN_{i,l_i}]$ and $PSN_{m-} \equiv SN^1_{j_1} \mid \cdots \mid SN^1_{j_m}$, $m \geq 1$ if $C_i \mid PSN_m \xrightarrow{\tau} C'_i \mid PSN'_{m'}$ we have that $C'_i \equiv GSS_{i,l_i}[SMS^3_{i,l_i} \mid SSN'_{i,l_i}]$, $SSN'_{i,l_i} \equiv SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_{l_i-1}}_{l_i-1} \mid SN^{h_{l_i}}_{i,l_i}$, and $\nu\, nid_{i,l_i}.SN^{h_{l_i}}_{i,l_i} \equiv \nu\, nid_{j_h}.\nu\, sr_{j_h}.SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}},\ ^{nid_{i,l_i}}/_{nid_{j_h}},\ ^{sr_{i,l_i}}/_{sr_{j_h}},\ ^{w_{i,l_i}}/_{w_{j_h}}\}$ for some $1 \leq h \leq m$ such that $SN^1_{j_h}$ occurs in PSN_m and $PSN'_{m'} \equiv SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN^1_{j_{h+1}} \mid \cdots \mid SN^1_{j_m}$. By definition of $\mathcal{R}$ we have that $D_i \equiv GMS_{i,l_i}[MMS^2_{i,l_i} \mid MSN_{i,l_i}]$, $MSN_{i,l_i} \equiv SSN_{i,l_i}$. We have that $D_i \mid PSN_m \equiv \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^2_{i,l_i} \mid MSN_{i,l_i} \mid !RMS_i \mid PSN_m) \equiv \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^2_{i,l_i} \mid SN^1_{j_h} \mid MSN_{i,l_i} \mid !RMS_i \mid PSN'_{m'}) \xrightarrow{\tau} \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.\nu\, nid_{j_h}.\nu\, sr_{j_h}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^3_{i,l_i} \mid SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}}\} \mid MSN_{i,l_i} \mid !RMS_i \mid PSN'_{m'}) \equiv \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i}.(MMS^7_{i,1} \mid \cdots \mid MMS^7_{i,l_i-1} \mid MMS^3_{i,l_i} \mid SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}},\ ^{nid_{i,l_i}}/_{nid_{j_h}},\ ^{sr_{i,l_i}}/_{sr_{j_h}},\ ^{w_{i,l_i}}/_{w_{j_h}}\} \mid MSN_{i,l_i} \mid !RMS_i \mid PSN'_{m'}) \equiv GMS_{i,l_i}[MMS^3_{i,l_i} \mid MSN'_{i,l_i}] \mid PSN'_{m'} \equiv D'_i \mid PSN'_{m'}$ where $MSN'_{i,l_i} \equiv SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_{l_i-1}}_{l_i-1} \mid SN^{h_{l_i}}_{i,l_i}$, $\nu\, nid_{i,l_i}.\nu\, sr_{i,l_i}.SN^{h_{l_i}}_{i,l_i} = \nu\, nid_{j_h}.\nu\, sr_{j_h}.SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}},\ ^{nid_{i,l_i}}/_{nid_{j_h}},\ ^{sr_{i,l_i}}/_{sr_{j_h}},\ ^{w_{i,l_i}}/_{w_{j_h}}\}$. Let $D' = \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN'_{m'} \mid !MSA\ !SN)$ we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA\ !SN) \equiv \nu\, dck.(D_i \mid PSN_m \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid !MSA\ !SN) \xrightarrow{\tau} \nu\, dck.(D'_i \mid PSN'_{m'} \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid !MSA\ !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN'_{m'} \mid !MSA\ !SN) = D'$ and $(C',\ D') \in \mathcal{R}$
- **(New MS)** $n' = n+1 \wedge C'_j = C'\ \forall j \neq n+1$, $C'_{n+1} = GSS_{n+1,1}[SMS^1_{n+1,1} \mid 0]$ and $PSN'_{m'} = PSN_m$. In this case the $!SSA$ component is unrolled and a new single session mobile station C'_{n+1} synchronizes with the *Init* process. if $SSA = \nu\, \widetilde{ss}_{n+1,1}.(Init_{n+1,1} \mid SMS^0_{n+1,1}) \xrightarrow{\tau} C'_{n+1} \equiv \nu\, \widetilde{ss}_{n+1,1}.SMS^1_{n+1,1} \equiv GSS_{n+1,1}[SMS^1_{n+1,1} \mid SSN_{n+1,1}]$, $SSN_{n+1,1} \equiv 0$. Let $D' = \nu\, dck.(D_1 \mid \cdots \mid D_n \mid D'_{n+1} \mid PSN_m \mid !MSA\ !SN)$ where $D'_{n+1} = GMS_{n+1,1}[MMS^1_{n+1,1} \mid MSN_{n+1,1}]$, $MSN_{n+1,1} \equiv 0$ then we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid !MSA\ !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid \nu\, \widetilde{ms}_{n+1,1}.(Init_{n+1,1} \mid MMS^0_{n+1,1}) \mid !MSA\ !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid \nu\, \widetilde{ms}_{n+1,1}.(Init_{n+1,1} \mid MMS^0_{n+1,1}) \mid PSN_m \mid !MSA\ !SN) \xrightarrow{\tau} \nu\, dck.(D_1 \mid \cdots \mid D_n \mid \nu\, \widetilde{ms}_{n+1,1}.(MMS^1_{n+1,1}) \mid PSN_m \mid !MSA\ !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid \nu\, \widetilde{ms}_{n+1,1}.(MMS^1_{n+1,1} \mid 0) \mid PSN_m \mid !MSA\ !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid D'_{n+1} \mid PSN_m \mid !MSA\ !SN) = D'$ and $(C',\ D') \in \mathcal{R}$

Let $(C,\ D) \in \mathcal{R}$ and let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid !PSN_m \mid !MSA \mid !SN)$ and $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid !PSN_m \mid !SSA \mid !SN)$.
If $C \xrightarrow{\tau} C'$ by Lemma 1 we have that $C' \equiv \nu\, dck.(C'_1 \mid \cdots \mid C'_{n'} \mid !PSN'_{m'} \mid !MSA \mid !SN)$ and we have 3 cases:

- $\exists i\ C_i \xrightarrow{\tau} C'_i \wedge C'_j = C_j\ \forall j \neq i \wedge n' = n \wedge PSN'_{m'} = PSN_m$, hence $C_i \equiv GMS_{i,l_i}[MMS^{k_{l_i}}_{i,l_i} \mid MSN_{i,l_i}]$ can do a silent transition this means that C_i is either of the form $C_i \equiv GMS_{i,l_i}[MMS^4_{i,l_i} \mid MSN_{i,l_i}]$ (i.e. we have two cases depending on the evaluation of the conditional statement), or of the form $C_i \equiv GMS_{i,l_i}[MMS^6_{i,l_i} \mid MSN_{i,l_i}]$ (i.e a new session of the mobile station is created). Hence we have 3 cases:
  - **(Conditional-then)** if $C_i \equiv GMS_{i,l_i}[MMS^4_{i,l_i} \mid MSN_{i,l_i}] \xrightarrow{\tau} GMS_{i,l_i}[MMS^5_{i,l_i} \mid MSN_{i,l_i}] = C'_i$ then $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i})) =_E$ TMSI_REALL i.e. $N_{i,l_i} =_E \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_REALL}, z_{i,l_i}))$. By definition of $\mathcal{R}$ we have that $D_i \equiv GSS_{i,l_i}[SMS^4_{i,l_i} \mid SSN_{i,l_i}]$, $SMS^4_{i,l_i} = SX_{i,l_i} \mid SChk_{i,l_i}\{^{N_{i,l_i}}/_{y_{i,l_i}}\}$ and $SChk_{i,l_i}\{^{N_{i,l_i}}/_{y_{i,l_i}}\} \equiv$ *if* $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i}))$ = TMSI_REALL *then* $\overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{COMPLETE})\rangle.\ \overline{d_{i,l_i}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i}))\rangle$ *else* $0 \equiv$ *if* $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_REALL}, z_{i,l_i}))))$ = TMSI_REALL *then* $\overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{COMPLETE})\rangle.\overline{d_{i,l_i}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,l_i}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_REALL}, z_{i,l_i}))))\rangle$ *else* $0 \xrightarrow{\tau} \overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{COMPLETE})\rangle.\overline{d_{i,l_i}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,j}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_REALL}, z_{i,l_i}))))\rangle$ hence $SMS^4_{i,l_i} \xrightarrow{\tau} SMS^5_{i,l_i}$ and $D_i \xrightarrow{\tau} SMS_{i,l_i}[SMS^5_{i,l_i} \mid SSN_{i,l_i}] = D'_i$ then let $D' = \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN)$ we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_i \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(D_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(D'_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) = D'$ and $(C',\ D') \in \mathcal{R}$
  - **(Conditional-else)** if $C_i \equiv GMS_{i,l_i}[MMS^4_{i,l_i} \mid MSN_{i,l_i}] \xrightarrow{\tau} GMS_{i,l_i}[MMS^8_{i,l_i} \mid MSN_{i,l_i}] = C'_i$ then $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i})) \neq_E$ TMSI_REALL i.e. $N_{i,l_i} \neq_E \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_REALL}, z_{i,l_i}))$. By definition of $\mathcal{R}$ we have that $D_i \equiv GSS_{i,l_i}[SMS^4_{i,l_i} \mid SSN_{i,l_i}]$, $SMS^4_{i,l_i} = SX_{i,l_i} \mid SChk_{i,l_i}\{^{N_{i,l_i}}/_{y_{i,l_i}}\}$ and $SChk_{i,l_i}\{^{N_{i,l_i}}/_{y_{i,l_i}}\} \equiv$ *if* $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i}))$ = TMSI_REALL *then* $\overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{COMPLETE})\rangle.\overline{d_{i,l_i}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,l_i}, N_{i,l_i}))\rangle$ *else* $0 \equiv$ *if* $\mathtt{fst}(\mathtt{sdec}(ck_{i,l_i}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_REALL}, z_{i,l_i}))))$ = TMSI_REALL *then* $\overline{up}\langle \mathtt{senc}(ck_{i,l_i}, mr_{i,l_i}, \text{COMPLETE})\rangle.$
    $\overline{d_{i,l_i}}\langle \mathtt{snd}(\mathtt{sdec}(ck_{i,l_i}, \mathtt{senc}(ck_{i,l_i}, sr_{i,l_i}, \mathtt{pair}(\text{TMSI\_REALL}, z_{i,l_i}))))\rangle$ *else* $0 \xrightarrow{\tau} 0$ hence $SMS^4_{i,l_i} \xrightarrow{\tau} SMS^8_{i,l_i}$ and $D_i \xrightarrow{\tau} SMS_{i,l_i}[SMS^8_{i,l_i} \mid SSN_{i,l_i}] = D'_i$ then let $D' = \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN)$ we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_i \mid \cdots \mid D_n \mid$

$PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(D_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(D'_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) = D'$ and $(C',\ D') \in \mathcal{R}$

– **(New session)** if $C_i \equiv GMS_{i,l_i}[MMS^6_{i,l_i} \mid MSN_{i,l_i}] \xrightarrow{\tau} D'_i \equiv GMS_{i,l_i+1}[MMS^1_{i,l_i+1} \mid MSN_{i,l_i+1}]$, $MSN_{i,l_i+1} \equiv MSN_{i,l_i} \mid 0$ then by definition of $\mathcal{R}$ we have that $D_i \equiv GSS_{i,l_i}[SMS^6_{i,l_i} \mid SSN_{i,l_i}]$ and $D_i \mid !SSA \equiv GSS_{i,l_i}[SMS^6_{i,l_i} \mid SSN_{i,l_i}] \mid \nu\, d_{i,l_i+1},\ id_{i,l_i+1},\ ck_{i,l_i+1}$ $\nu\, mr_{i,l_i+1}.(Init_{i,l_i+1} \mid SMS^0_{i,l_i+1}) \mid !SSA \xrightarrow{\tau} GSS_{i,l_i}[SMS^6_{i,l_i} \mid SSN_{i,l_i}] \mid \nu\, d_{i,l_i+1},\ id_{i,l_i+1},\ ck_{i,l_i+1}.\nu\, mr_{i,l_i+1}.(SMS^1_{i,l_i+1}) \mid !SSA \equiv \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,l_i} \mid SSN_{i,l_i}) \mid \nu\, d_{i,l_i+1},\ id_{i,l_i+1},\ ck_{i,l_i+1}.\nu\, mr_{i,l_i+1}.(SMS^1_{i,l_i+1}) \mid !SSA \equiv \nu\, \widetilde{ss}_{i,l_i+1}.\nu\, \widetilde{nid}_{i,l_i}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,l_i} \mid SMS^1_{i,l_i+1} \mid SSN_{i,l_i} \mid 0) \mid !SSA \equiv GSS_{i,l_i+1}[SMS^1_{i,l_i+1} \mid SSN_{i,l_i+1}] \mid !SSA = C'_i \mid !SSA$ Let $D' = \nu\, dck.(D_1 \mid \cdots \mid D'_{n'} \mid PSN_m \mid !SSA \mid !SN)$, we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_i \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(SSA \mid D_1 \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(D'_{n'} \mid D_1 \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D'_{n'} \mid PSN_m \mid !SSA \mid !SN) = D'$ and $(C',\ D') \in \mathcal{R}$

- **(MS/SN synch)** $\exists i\ C_i \mid PSN_m \xrightarrow{\tau} C'_i \mid PSN'_{m'} \wedge C'_j = C_j\ \forall j \neq i \wedge n' = n$ the only possible silent transition between C_i and PSN_m is the communication on the channel dck hence, $C_i \equiv GMS_{i,l_i}[MMS^2_{i,l_i} \mid MSN_{i,l_i}]$ and $PSN_{m-} \equiv SN^1_{j_1} \mid \cdots \mid SN^1_{j_m}$, $m \geq 1$ if $C_i \mid PSN_m \xrightarrow{\tau} C'_i \mid PSN'_{m'}$ we have that $C'_i \equiv GMS_{i,l_i}[MMS^3_{i,l_i} \mid MSN'_{i,l_i}]$, $MSN'_{i,l_i} \equiv SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_{l_i-1}}_{l_i-1} \mid SN^{h_{l_i}}_{i,l_i}$, and $\nu\, nid_{i,l_i}.SN^{h_{l_i}}_{i,l_i} \equiv \nu\, nid_{j_h}.\nu\, sr_{j_h}.SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}},\ ^{nid_{i,l_i}}/_{nid_{j_h}},\ ^{sr_{i,l_i}}/_{sr_{j_h}},\ ^{w_{i,l_i}}/_{w_{j_h}}\}$ for some $1 \leq h \leq m$ such that $SN^1_{j_h}$ occurs in PSN_m and $PSN'_{m'} \equiv SN^1_{j_1} \mid \cdots \mid SN^1_{j_{h-1}} \mid SN^1_{j_{h+1}} \mid \cdots \mid SN^1_{j_m}$. By definition of $\mathcal{R}$ we have that $D_i \equiv GSS_{i,l_i}[SMS^2_{i,l_i} \mid SSN_{i,l_i}]$, $SSN_{i,l_i} \equiv MSN_{i,l_i}$. We have that $D_i \mid PSN_m \equiv \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,l_i-1} \mid SMS^2_{i,l_i} \mid SSN_{i,l_i} \mid PSN_m) \equiv \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,l_i-1} \mid SMS^2_{i,l_i} \mid SN^1_{j_h} \mid SSN_{i,l_i} \mid PSN'_{m'}) \xrightarrow{\tau} \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i-1}.\nu\, nid_{j_h}.\nu\, sr_{j_h}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,l_i-1} \mid SMS^3_{i,l_i} \mid SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}}\} \mid SSN_{i,l_i} \mid PSN'_{m'}) \equiv \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,l_i}.(SMS^7_{i,1} \mid \cdots \mid SMS^7_{i,l_i-1} \mid SMS^3_{i,l_i} \mid SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}},\ ^{nid_{i,l_i}}/_{nid_{j_h}},\ ^{sr_{i,l_i}}/_{sr_{j_h}},\ ^{w_{i,l_i}}/_{w_{j_h}}\} \mid SSN_{i,l_i} \mid PSN'_{m'}) \equiv GSS_{i,l_i}[SMS^3_{i,l_i} \mid SSN'_{i,l_i}] \mid PSN'_{m'} \equiv D'_i \mid PSN'_{m'}$ where $SSN'_{i,l_i} \equiv SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_{l_i-1}}_{l_i-1} \mid SN^{h_{l_i}}_{i,l_i}$, $\nu\, nid_{i,l_i}.\nu\, sr_{i,l_i}.SN^{h_{l_i}}_{i,l_i} = \nu\, nid_{j_h}.\nu\, sr_{j_h}.SN^2_{j_h}\{^{ck_{i,l_i}}/_{xck_{j_h}},\ ^{nid_{i,l_i}}/_{nid_{j_h}},\ ^{sr_{i,l_i}}/_{sr_{j_h}},\ ^{w_{i,l_i}}/_{w_{j_h}}\}$. Let $D' = \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN'_{m'} \mid !SSA \mid !SN)$ we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_i \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(D_i \mid PSN_m \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid !SSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(D'_i \mid PSN'_{m'} \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid !SSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN'_{m'} \mid !SSA \mid !SN) = D'$ and $(C',\ D') \in \mathcal{R}$
- **(New MS)** $n' = n+1 \wedge C'_j = C'\ \forall j \neq n+1$, $C'_{n+1} = GMS_{n+1,1}[MMS^1_{n+1,1} \mid 0]$ and $PSN'_{m'} = PSN_m$. In this case the $!MSA$ component is unrolled and a new single session mobile station C'_{n+1} synchronizes with the $Init$ process. if $MSA = \nu\, \widetilde{ms}_{n+1,1}.(Init_{n+1,1} \mid MMS^0_{n+1,1}) \xrightarrow{\tau} C'_{n+1} \equiv \nu\, \widetilde{ms}_{n+1,1}.MMS^1_{n+1,1} \equiv GMS_{n+1,1}[MMS^1_{n+1,1} \mid MSN_{n+1,1}]$, $MSN_{n+1,1} \equiv 0$. Let $D' = \nu\, dck.(D_1 \mid \cdots \mid D_n \mid D'_{n+1} \mid PSN_m \mid !SSA \mid !SN)$ where $D'_{n+1} = GSS_{n+1,1}[SMS^1_{n+1,1} \mid SSN_{n+1,1}]$, $SSN_{n+1,1} \equiv 0$ then we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid \nu\, \widetilde{ss}_{n+1,1}.(Init_{n+1,1} \mid SMS^0_{n+1,1}) \mid !SSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid \nu\, \widetilde{ss}_{n+1,1}.(Init_{n+1,1} \mid SMS^0_{n+1,1}) \mid PSN_m \mid !SSA \mid !SN) \xrightarrow{\tau} \nu\, dck.(D_1 \mid \cdots \mid D_n \mid \nu\, \widetilde{ss}_{n+1,1}.(SMS^1_{n+1,1}) \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid \nu\, \widetilde{ss}_{n+1,1}.(SMS^1_{n+1,1} \mid 0) \mid PSN_m \mid !SSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid D'_{n+1} \mid PSN_m \mid !MSA \mid !SN) = D'$ and $(C',\ D') \in \mathcal{R}$

Let $(C,\ D) \in \mathcal{R}$ and let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid !PSN_m \mid !SSA \mid !SN)$ and $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid !PSN_m \mid !MSA \mid !SN)$. If $C \xrightarrow{\alpha} C'$ then by Lemma 2 we have 2 cases:

- $\exists i\ C_i \xrightarrow{\alpha} C'_i \wedge C'_j = C_j\ \forall j \neq i \wedge n' = n \wedge PSN'_{m'} = PSN_m$ in this case one of the C_i components does the transition. We have 2 cases:

  – **(Active session MS α-transition)** if $C_i = GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}] \xrightarrow{\alpha} C'_i \equiv GSS_{i,l_i}[SMS^{k_i+1}_{i,l_i} \mid SSN_{i,l_i}], k \neq 2,4$ then we have 3 cases:

    i) if $k_i = 1$, $SMS^{k_i}_{i,l_i} = SMS^1_{i,l_i} \xrightarrow{\nu x_{i,l_i}.\overline{up}\langle x_{i,l_i}\rangle} SMS^2_{i,l_i} = SMS^{k_i+1}_{i,l_i}$, then by definition of $\mathcal{R}$ we have that $MMS^{k_i}_{i,l_i} = MMS^1_{i,l_i} \xrightarrow{\nu x_{i,l_i}.\overline{up}\langle x_{i,l_i}\rangle} MMS^2_{i,l_i} = MMS^{k_i+1}_{i,l_i}$, hence $D_i = GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}] \xrightarrow{\nu x_{i,l_i}.\overline{up}\langle x_{i,l_i}\rangle} GMS_{i,l_i}[MMS^{k_i+1}_{i,l_i} \mid MSN_{i,l_i}] = D'_i$

    ii) if $k_i = 3$, $SMS^{k_i}_{i,l_i} = SMS^3_{i,l_i} \xrightarrow{dw(N_{i,l_i})} SMS^4_{i,l_i} = SMS^{k_i+1}_{i,l_i}$, then by definition of $\mathcal{R}$ we have that $MMS^{k_i}_{i,l_i} = MMS^3_{i,l_i} \xrightarrow{dw(N_{i,l_i})} MMS^4_{i,l_i} = MMS^{k_i+1}_{i,l_i}$ hence $GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}] \xrightarrow{dw(N_{i,l_i})} GMS_{i,l_i}[MMS^{k_i+1}_{i,l_i} \mid MSN_{i,l_i}] = D'_i$

    iii) if $k_i = 5$, $SMS^{k_i}_{i,l_i} = SMS^5_{i,l_i} \xrightarrow{\nu k_{i,l_i}.\overline{up}\langle k_{i,l_i}\rangle} SX_{i,l_i} \mid SK_{i,l_i} \mid \overline{d_{i,l_i}}\langle \mathsf{snd}(sdec(ck_{i,l_i},\ N_{i,l_i}))\rangle = SMS^{k_i+1}_{i,l_i}$. By definition of $\mathcal{R}$ we have that $MMS^{k_i}_{i,l_i} \equiv MMS^6_{i,l_i} \xrightarrow{\nu k_{i,l_i}.\overline{up}\langle k_{i,l_i}\rangle} MX_{i,l_i} \mid MK_{i,l_i} \mid \overline{d_{i,1}}\langle \mathsf{snd}(sdec(ck_{i,l_i},\ N_{i,l_i}))\rangle = MMS^{k_i+1}_{i,l_i}$, hence $D_i \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}] \xrightarrow{\nu k_{i,l_i}.\overline{up}\langle k_{i,l_i}\rangle} GMS_{i,l_i}[MMS^{k_i+1}_{i,l_i} \mid MSN_{i,l_i}] = D'_i$

    Let $D' = \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN)$ where $D'_i = GMS_{i,l_i}[MMS^{k_i+1}_{i,l_i} \mid MSN_{i,l_i}]$ as shown in the cases above, then we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(D_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\alpha} \nu\, dck.(D'_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) = D'$ and $(C',\ D') \in \mathcal{R}$

– **(SN post-synch α-transition)** if $C_i \equiv GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}] \xrightarrow{\alpha} C'_i \equiv GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN'_{i,l_i}]$ for some $1 \leq j \leq l_i$ such that $SSN_{i,l_i} \equiv SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_j}_{i,j} \mid \cdots \mid SN^{h_{l_i}}_{i,l_i} \xrightarrow{\alpha} SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_j+1}_{i,j} \mid \cdots \mid SN^{h_{l_i}}_{i,l_i} = SSN'_{i,l_i}$ and $h_j \in \{2,3\}$ then by definition of $\mathcal{R}$ we have that $D_i \equiv GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}]$ and $MSN_{i,l_i} \equiv SSN_{i,l_i} \overset{S}{S} N'_{i,l_i} = MSN_{i,l_i}$ then $D_i \xrightarrow{\alpha} GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN'_{i,l_i}] = D'_i$ where $MSN'_{i,l_i} = SSN'_{i,l_i}$. Let $D' = \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN)$ then we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(D_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{\alpha} \nu\, dck.(D'_i \mid D_1 \mid \cdots \mid D_{i-1} \mid D_{i+1} \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D'_i \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) = D'$ and $(C',\ D') \in \mathcal{R}$

- **(SN pre-synch α-transition)** $C'_j = C_j\ \forall \wedge n' = n \wedge PSN'_{m'} = PSN_m \mid SN^1_{j_{m+1}},\ m' = m+1$. In this case a new SN is unrolled and does the first labelled transition before synchronizing with the MS. If $!SN \xrightarrow{\alpha} SN^1_{j_{m+1}} \mid !SN$ and $C' \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_{m+1} \mid !SSA \mid !SN), PSN_{m+1} \equiv PSN_m \mid SN^1_{j_{m+1}}$ then let $D' \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_{m+1} \mid !MSA \mid !SN)$, where $PSN_{m+1} \equiv PSN_m \mid SN^1_{j_{m+1}}$, we have that $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN \mid SN^0_{j_{m+1}}) \equiv \nu\, dck.(SN^0_{j_{m+1}} \mid D_1 \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \xrightarrow{dw(z_{j_{m+1}})} \nu\, dck.(SN^1_{j_{m+1}} \mid D_1 \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN) \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid SN^1_{j_{m+1}} \mid !MSA \mid !SN) = D'$, and $(C',\ D') \in \mathcal{R}$

Let $(C,\ D) \in \mathcal{R}$ and let $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !MSA \mid !SN)$ and $D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid !SSA \mid !SN)$.
Analogous to the previous case

□

C. PROOF OF LEMMA 5

In order to prove Lemma 5, we define the general structure of the frames produced by partial evolution of our processes through the following substitutions:

$$
\begin{array}{lll}
\sigma^{id}_{i,j} & \overset{def}{=} & \{^{id_{i,1}}/_{x_{i,1}}, {}^{id_{i,2}}/_{x_{i,2}}, \ldots,\ {}^{id_{i,j}}/_{x_{i,j}}\} \\
\sigma^{M}_{i,j} & \overset{def}{=} & \{^{id_{i,1}}/_{x_{i,1}}, {}^{M_{i,2}}/_{x_{i,2}} \ldots,\ {}^{M_{i,j}}/_{x_{i,j}}\} \\
\sigma^{K}_{i,j} & \overset{def}{=} & \{^{\mathtt{senc}(ck_{i,1},\ mr_{i,1},\ \textsc{Complete})}/_{k_{i,1}}, \ldots,\ {}^{\mathtt{senc}(ck_{i,j},\ mr_{i,j},\ \textsc{Complete})}/_{k_{i,j}}\} \\
\sigma^{nid}_{i,j} & \overset{def}{=} & \{^{\mathtt{senc}(ck_{i,1},\ sr_{i,1},\ \mathtt{pair}(\textsc{TMSI\_Reall},\ nid_{i,1}))}/_{y_{i,1}}, \ldots, {}^{\mathtt{senc}(ck_{i,j},\ sr_{i,j},\ \mathtt{pair}(\textsc{TMSI\_Reall},\ nid_{i,j}))}/_{y_{i,j}}\}
\end{array}
$$

We define the general structure of the frame of one of the grouped single (resp. multi)-session system components

$$
\begin{array}{lll}
\sigma(C_i) & \overset{def}{=} & \sigma^{id}_{i,j_{id}} \mid \sigma^{K}_{i,j_K} \mid \sigma^{nid}_{i,j_{nid}} \\
\sigma(D_i) & \overset{def}{=} & \sigma^{M}_{i,j_{id}} \mid \sigma^{K}_{i,j_K} \mid \sigma^{nid}_{i,j_{nid}}
\end{array}
$$

These frames represent the knowledge a grouped single (resp. multi)-session system component releases to the environment after $i + l_i - 1$ mobile stations completely executed (resp. the i^{th} MS completely executed $l_i - 1$ sessions of) the TMSI reallocation protocol while the l^{th}_i executed k_{l_i} steps (resp. while the l_i session is at the k_{l_i} execution step).

In the following lemma we prove the correctness of the given frame structure.

Lemma 4. *Let* $(C,D) \in \mathcal{R}, C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN), D \equiv \nu\, dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN)$ *then* $\varphi(C) \equiv \nu\, dck.(\varphi(C_1) \mid \cdots \mid \varphi(C_n)),\ \varphi(D) \equiv \nu\, dck.(\varphi(D_1) \mid \cdots \mid \varphi(D_n))$ *and* $\forall i,\ l_i, 1 \leq i \leq n, l_i \geq 1$,

$$
\begin{array}{lll}
\varphi(C_i) & \equiv & \varphi(GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}]) \\
 & \equiv & \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,j_{nid}}.\sigma(C_i) = \nu\, \widetilde{ss}_{i,l_i}.\nu\, \widetilde{nid}_{i,j_{nid}}.(\sigma^{id}_{i,j_{id}} \mid \sigma^{K}_{i,j_K} \mid \sigma^{nid}_{i,j_{nid}}) \\
\varphi(D_i) & \equiv & \varphi(GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}]) \\
 & \equiv & \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,j_{nid}}.\sigma(D_i) = \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,j_{nid}}.(\sigma^{M}_{i,j_{id}} \mid \sigma^{K}_{i,j_K} \mid \sigma^{nid}_{i,j_{nid}})
\end{array}
$$

where $j_{id} = \begin{cases} l_i - 1 & \text{if } k_i \leq 1 \\ l_i & \text{otherwise} \end{cases}$ $j_K = \begin{cases} l_i - 1 & \text{if } k_i \leq 5, k_i = 8 \\ l_i & \text{otherwise} \end{cases}$ $j_{nid} = \begin{cases} l_i - 1 & \text{if } k_i \leq 2 \\ l_i & \text{otherwise} \end{cases}$

Proof. By definition of PSN_m, PSN_m we have that $\varphi(PSN_m) \equiv \varphi(PSN_m) \equiv 0,\ \forall\, m \geq 0$ and by definition of $SSA,\ MSA$ and SN we have that $\varphi(!SSA) \equiv \varphi(!MSA) \equiv \varphi(!SN) \equiv 0$.
By definition of $\mathcal{R}$ we have that $C \equiv \nu\, dck.(C_1 \mid \cdots \mid C_n \mid PSN_m \mid !SSA \mid !SN), D \equiv \nu\ dck.(D_1 \mid \cdots \mid D_n \mid PSN_m \mid !MSA \mid !SN)$ and $\varphi(C) \equiv \nu\, dck.(\varphi(C_1) \mid \cdots \mid \varphi(C_n)),\ \varphi(D) \equiv \nu\, dck.(\varphi(D_1) \mid \cdots \mid \varphi(D_n))$. We show by induction over l_i that
$\varphi(C_i) \equiv \nu\, \widetilde{ss_{i,l_i}}.\nu\, \widetilde{nid}_{i,j_{nid}}.(\sigma^{id}_{i,j_{id}} \mid \sigma^{K}_{i,j_K} \mid \sigma^{nid}_{i,j_{nid}})$,
$\varphi(D_i) \equiv \nu\, \widetilde{ms_{i,l_i}}.\nu\, \widetilde{nid}_{i,j_{nid}}.(\sigma^{M}_{i,j_{id}} \mid \sigma^{K}_{i,j_K} \mid \sigma^{nid}_{i,j_{nid}})$
where $C_i = GSS_{i,l_i}[SMS^{k_i}_{i,l_i} \mid SSN_{i,l_i}],\ D_i = GMS_{i,l_i}[MMS^{k_i}_{i,l_i} \mid MSN_{i,l_i}]$ and $j_{id} = \begin{cases} l_i - 1 & \text{if } k_i \leq 1 \\ l_i & \text{otherwise} \end{cases}$ $j_K = \begin{cases} l_i - 1 & \text{if } k_i \leq 5, k_i = 8 \\ l_i & \text{otherwise} \end{cases}$
$j_{nid} = \begin{cases} l_i - 1 & \text{if } k_i \leq 2 \\ l_i & \text{otherwise} \end{cases}$

- $l_i = 0$). We prove the statements hold for $l_i = 0$. Let $l_i = 0$, by definition of $\mathcal{R}, C_i \equiv GSS_{i,0}[SMS^{k_i}_{i,0} \mid SSN_{i,0}] \equiv 0,\ D_i \equiv GMS_{i,0}[MMS^{k_1}_{i,0} \mid MSN_{i,0}] \equiv 0\ \varphi(C_i) \equiv 0 \equiv \varphi(D_i)$

- $l_i = m + 1$). We assume the statement holds for $l_i = m$, and show that it holds for $l_i = m + 1$ i.e.
$\varphi(C_i) \equiv \varphi(GSS_{i,m+1}[SMS^{k_{m+1}}_{i,m+1} \mid SSN_{i,m+1}]) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,j'_{id}} \mid \sigma^{K}_{i,j'_K+1} \mid \sigma^{nid}_{i,j'_{nid}+1}),\ \varphi(D_i) \equiv \varphi(GMS_{i,m+1}[MMS^{k_{m+1}}_{i,m+1} \mid MSN_{i,m+1}] \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,j'_{id}} \mid \sigma^{K}_{i,j'_K} \mid \sigma^{nid}_{i,j'_{nid}}),$ where

$j'_{id} = \begin{cases} m & \text{if } k_{m+1} \leq 1 \\ m+1 & \text{otherwise} \end{cases}$ $j'_K = \begin{cases} m & \text{if } k_{m+1} \leq 5, \text{ or } k_{m+1} = 8 \\ m+1 & \text{otherwise} \end{cases}$ $j'_{nid} = \begin{cases} m & \text{if } k_{m+1} \leq 2 \\ m+1 & \text{otherwise} \end{cases}$

Let $l_i = m + 1$, by definition of $\mathcal{R}$, we have that $C_i \equiv GSS_{i,m+1}[SMS^{k_{m+1}}_{i,m+1} \mid SSN_{i,m+1}],\ D_i \equiv GMS_{i,m+1}[MMS^{k_{m+1}}_{i,m+1} \mid MSN_{i,m+1}]$ where $GSS_{i,m+1}[] = \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(SMS^{7}_{i,1} \mid \cdots \mid SMS^{7}_{i,m} \mid \_) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(SMS^{7}_{i,1} \mid \cdots \mid SMS^{7}_{i,m-1} \mid SMS^{7}_{i,m} \mid \_) \equiv \nu\, id_{i,m+1}, d_{i,m+1}, ck_{i,m+1}.\nu\, nid_{i,j'_{nid}}.(GSS_{i,m}[SMS^{7}_{i,m}] \mid [\_])$ and
$GMS_{i,m+1}[] = \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{1,j'_{nid}}.(MMS^{7}_{i,1} \mid \cdots \mid MMS^{7}_{i,m} \mid \_ \mid !R_i) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{1,j'_{nid}}.(MMS^{7}_{i,1} \mid \cdots \mid MMS^{7}_{i,m-1} \mid MMS^{7}_{i,m} \mid \_ \mid !R_i) \equiv \nu\, ck_{i,m+1}.\nu\, nid_{i,j'_{nid}}.(GMS_{i,m}[MMS^{7}_{1,m} \mid \_])$ then
$\varphi(C_i) \equiv \varphi(GSS_{i,m+1}[SMS^{k_{m+1}}_{i,m+1} \mid SSN_{i,m+1}]) \equiv \varphi(GSS_{i,m}[SMS^{7}_{i,m} \mid SSN_{i,m}]) \mid \nu\, id_{i,m+1}, d_{i,m+1}, ck_{i,m+1}.\nu\, nid_{i,m+1}.\varphi(SMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1}) \equiv$ (by ind. hyp. and since $\varphi(MMS^{7}_{i,j}) \equiv MX_{i,j} \mid K_{i,j} \forall i, j$ and since the conditional enables the process $SMS^{k_j}_{i,j}$ to reach state 7 if and only if it receives $sdec(ck_{i,j}, \texttt{pair}(\text{TMSI\_REALL}, nid_{i,j}$ from the $SN_{i,j}$ we have that $SSN_{i,m} \equiv SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_m}_{i,m}$ with $h_1, \ldots, h_m \geq 3$ hence $\varphi(SSN_{i,m}) \equiv \sigma^{nid}_{i,m})\ \nu\, \widetilde{ss}_{i,m}.\nu\, \widetilde{nid}_{i,m}.(\sigma^{id}_{i,m} \mid \sigma^{k}_{i,m} \mid \sigma^{nid}_{i,m}) \mid \nu\, id_{i,m+1}, d_{i,m+1}, ck_{i,m+1}, nid_{i,j'_{nid}}.\varphi(SMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1})) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m} \mid \sigma^{k}_{i,m} \mid \sigma^{nid}_{i,m} \mid \varphi(SMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1}))$ and
$\varphi(D_i) \equiv \varphi(GMS_{i,m+1}[MMS^{k_{m+1}}_{i,m+1} \mid MSN_{i,m+1}]) \equiv \varphi(GMS_{i,m}[MMS^{7}_{i,m} \mid MSN_{i,m} \mid \varphi(\nu\, ck_{i,m+1}, nid_{i,j'_{nid}}.(MMS^{k_{m+1}}_{1,m+1} \mid SN^{h_{m+1}}_{1,m+1})]) \equiv$(since $\varphi(MMS^{7}_{i,j}) \equiv MX_{i,j} \mid K_{i,j} \forall i, j$ since the conditional enables the process $SMS^{k_j}_{i,j}$ to reach state 7 if and only if it receives $sdec(ck_{i,j}, \texttt{pair}(\text{TMSI\_REALL}, nid_{i,j}$ from the $SN_{i,j}$ we have that $MSN_{i,m} \equiv SN^{h_1}_{i,1} \mid \cdots \mid SN^{h_m}_{i,m}$ with $h_1, \ldots, h_m \geq 3$ hence $\varphi(MSN_{i,m}) \equiv \sigma^{nid}_{i,m}$ and by ind. hyp. $\varphi(GMS_{i,m}[MMS^{7}_{i,m} \mid MSN_{i,m}]) \equiv \nu\, \widetilde{ms}_{i,m}.\nu\, \widetilde{nid}_{i,m}.(\sigma^{M}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m}))\ \nu\, \widetilde{ms}_{i,m}.\nu\, \widetilde{nid}_{i,m}.(\sigma^{M}_{i,m} \mid \sigma^{k}_{i,m} \mid \sigma^{nid}_{i,m} \mid \nu\, ck_{i,m+1}, \nu\, nid_{i,j'_{nid}}.\varphi(MMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1})) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m} \mid \sigma^{k}_{i,m} \mid \sigma^{nid}_{i,m} \mid \varphi(MMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1}))$
we have 6 cases:

1. $k_{m+1} = 1,\ SN^{h_{m+1}}_{i,m+1} = 0$ then we have that $\varphi(SMS^{1}_{i,m+1} \mid 0) \equiv 0$, hence $\varphi(C_i) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid 0) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,j'_{id}} \mid \sigma^{K}_{i,j'_K} \mid \sigma^{nid}_{i,j'_{nid}})$ and $\varphi(MMS^{1}_{i,m+1} \mid 0) \equiv 0$, hence, $\varphi(D_i) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid 0) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,j'_{id}} \mid \sigma^{K}_{i,j'_K} \mid \sigma^{nid}_{i,j'_{nid}})$
2. $k_{m+1} = 2,\ SN^{h_{m+1}}_{i,m+1} = 0$ then we have that
$\varphi(SMS^{2}_{i,m+1} \mid 0) \equiv SX_{i,m+1}$, hence, $\varphi(C_i) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid \{^{id_{i,m+1}}/_{x_{i,m+1}}\}) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m+1} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m})$ and
$\varphi(MMS^{2}_{i,m+1} \mid 0) \equiv MX_{i,m+1}$, hence, $\varphi(D_i) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,m}.(\sigma^{M}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid \{^{M_{i,m+1}}/_{x_{i,m+1}}\}) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m+1} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m}),\ j'_{nid} = m$
3. $k_{m+1} \in \{3, 4, 5, 8\},\ h_{m+1} = 2$ then we have that
$\varphi(SMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1}) \equiv \{^{id_{i,m+1}}/_{x_{i,m+1}}\}\}$, hence $\varphi(C_i) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid \{^{id_{i,m+1}}/_{x_{i,m+1}}\}) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m+1} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m})$ and
$\varphi(MMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1}) \equiv \{^{M_{i,m+1}}/_{x_{i,m+1}}\}$, hence $\varphi(D_i) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m}) \mid \{^{M_{i,m+1}}/_{x_{i,m+1}}\}) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m+1} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m}),\ j'_{nid} = m + 1$
4. $k_{m+1} \in \{3, 4, 5, 8\},\ h_{m+1} \in \{3, 4\}$ then we have that
$\varphi(SMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1}) \equiv \{^{id_{i,m+1}}/_{x_{i,m+1}}\} \mid \{^{\text{senc}(ck_{i,m+1}, sr_{i,m+1}, \texttt{pair}(\text{TMSI\_REALL}, nid_{i,m+1}))}/_{y_{i,m+1}}\}$, hence $\varphi(C_i) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m} \mid \sigma^{K}_{i,m} \mid$

$\sigma^{nid}_{i,m} \mid \{^{id_{i,m+1}}/_{x_{i,m+1}}\} \mid \{^{\mathtt{senc}(ck_{i,m+1},sr_{i,m+1},\mathtt{pair}(\text{TMSI\_REALL},nid_{i,m+1}))}/_{y_{i,m+1}}\}) \equiv, \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m+1} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m+1})$ and
$\varphi(MMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1}) \equiv \{^{M_{i,m+1}}/_{x_{i,m+1}}\} \mid \{^{\mathtt{senc}(ck_{i,m+1},sr_{i,m+1},\mathtt{pair}(\text{TMSI\_REALL},nid_{i,m+1}))}/_{y_{i,m+1}}\}$, hence $\varphi(D_i) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid \{^{M_{i,m+1}}/_{x_{i,m+1}}\} \mid \{^{\mathtt{senc}(ck_{i,m+1},sr_{i,m+1},\mathtt{pair}(\text{TMSI\_REALL},nid_{i,m+1}))}/_{y_{i,m+1}}\}) \equiv \nu\, dck.\nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m+1} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m+1}),\ j'_{nid} = m+1$

5. $k_{m+1} \in \{6,\ 7\},\ h_{m+1} = 2$ then we have that
$\varphi(SMS^{k_{m+1}}_{i,m+1} \mid SN^{2}_{i,m+1}) \equiv \{^{id_{i,m+1}}/_{x_{i,m+1}}\} \mid SK_{i,m+1})$, hence $\varphi(C_i) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid \{^{id_{i,m+1}}/_{x_{i,m+1}}\} \mid SK_{i,m+1}) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m+1} \mid \sigma^{K}_{i,m+1} \mid \sigma^{nid}_{i,m})$ and
$\varphi(MMS^{k_{m+1}}_{i,m+1} \mid SN^{2}_{i,m+1}) \equiv \{^{M_{i,m+1}}/_{x_{i,m+1}}\} \mid MK_{i,m+1}$, hence $\varphi(D_i) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid \{^{M_{i,m+1}}/_{x_{i,m+1}}\} \mid MK_{i,m+1}) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m+1} \mid \sigma^{K}_{i,m+1} \mid \sigma^{nid}_{i,m}),\ j'_{nid} = m+1$
6. $k_{m+1} \in \{6,\ 7\},\ h_{m+1} \in \{3, 4\}$ then we have that
$\varphi(SMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1}) \equiv \{^{id_{i,m+1}}/_{x_{i,m+1}}\} \mid SK_{i,m+1} \mid \nu\, nid_{i,m+1}.\{^{\mathtt{senc}(ck_{i,m+1},sr_{i,m+1},\mathtt{pair}(\text{TMSI\_REALL},nid_{i,m+1}))}/_{y_{i,m+1}}\}$, hence $\varphi(C_i) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid \{^{id_{i,m+1}}/_{x_{i,m+1}}\} \mid SK_{i,m+1} \mid \nu\, nid_{i,m+1}.\{^{\mathtt{senc}(ck_{i,m+1},sr_{i,m+1},\mathtt{pair}(\text{TMSI\_REALL},nid_{i,m+1}))}/_{y_{i,m+1}}\}) \equiv \nu\, \widetilde{ss}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{id}_{i,m+1} \mid \sigma^{K}_{i,m+1} \mid \sigma^{nid}_{i,m+1})$ and
$\varphi(MMS^{k_{m+1}}_{i,m+1} \mid SN^{h_{m+1}}_{i,m+1}) \equiv \{^{M_{i,m+1}}/_{x_{i,m+1}}\} \mid MK_{i,m+1} \mid \nu\, nid_{i,m+1}.\{^{\mathtt{senc}(ck_{i,m+1},sr_{i,m+1},\mathtt{pair}(\text{TMSI\_REALL},nid_{i,m+1}))}/_{y_{i,m+1}}\}$, hence $\varphi(D_i) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m} \mid \sigma^{K}_{i,m} \mid \sigma^{nid}_{i,m} \mid \{^{M_{i,m+1}}/_{x_{i,m+1}}\} \mid MK_{i,m+1} \mid \nu\, nid_{i,m+1}.\{^{\mathtt{senc}(ck_{i,m+1},sr_{i,m+1},\mathtt{pair}(\text{TMSI\_REALL},nid_{i,m+1}))}/_{y_{i,m+1}}\}) \equiv \nu\, \widetilde{ms}_{i,m+1}.\nu\, \widetilde{nid}_{i,j'_{nid}}.(\sigma^{M}_{i,m+1} \mid \sigma^{K}_{i,m+1} \mid \sigma^{nid}_{i,m+1}),\ j'_{nid} = m+1$

□

We can now prove Lemma 5

LEMMA 5. *If $(C, D) \in \mathcal{R}$ then $C \approx_s D$*

PROOF. by Lemma 4 we have that $\forall\ (C, D) \in \mathcal{R},\ \varphi(C) \equiv \nu\, dck.(\varphi(C_1) \mid \cdots \mid \varphi(C_n)),\ \varphi(D) \equiv \nu\, dck.(\varphi(D_1) \mid \cdots \mid \varphi(D_n))$. By lemma 4 we have that $\forall i,\ j,\ 1 \le i \le n,\ 1 \le j \le l_i, \varphi(D_i) = \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,j_{nid}}.(\sigma^{M}_{i,j_{id}} \mid \sigma^{K}_{i,j_K} \mid \sigma^{nid}_{i,j_{nid}})$ and by definition $\sigma^{M}_{i,j_{id}} = \{^{id_{i,1}}/_{x_{i,1}},\ ^{M_{i,2}}/_{x_{i,2}} \ldots,\ ^{M_{i,j_{id}}}/_{x_{i,j_{id}}}\}$. We show that $\forall i,\ j,\ 1 \le i \le n,\ 1 \le j \le l_i\ M_{i,j} \rightarrow nid_{i,j-1}$. By definition of the process D we have that $M_{i_j} =_E snd(sdec(ck_{i,j-1}, N_{i,j-1}))$. Hence $M_{i_j} \rightarrow^* nid_{i,j-1}$ if $N_{i,j-1} =_E \mathtt{senc}(ck_{i,j-1}, sr_{i,j-1}, (\text{TMSI\_REALL}, nid_{i,j-1}))$ and $M_{i_j} \rightarrow^* snd(sdec(ck_{i,j-1}, N_{i,j-1}\downarrow))$ otherwise. By contradiction let assume that $M_{i,j} \neq_E nid_{i,j-1}$ then $N_{i,j-1} \neq_E \mathtt{senc}(ck_{i,j-1}, sr_{i,j-1}, (\text{TMSI\_REALL}, nid_{i,j-1}))$ we have 3 cases:

- $N_{i,j-1} \neq_E \mathtt{senc}(T_{i,j-1}, U_{i,j-1}, L_{i,j-1})$ then $fst(sdec(ck_{i,j-1}, N_{i,j-1})) \neq_E$ TMSI_REALL and the if check fails so $M_{i,j}$ is not outputted at all;
- $N_{i,j-1} =_E \mathtt{senc}(T_{i,j-1}, U_{i,j-1}, L_{i,j-1})$ and $T_{i,j-1} \neq_E ck_{i,j-1}$ then $fst(sdec(ck_{i,j-1}, N_{i,j-1})) \neq_E$ TMSI_REALL and the if check fails so $M_{i,j}$ is not outputted at all;
- $N_{i,j-1} \neq_E \mathtt{senc}(T_{i,j-1}, U_{i,j-1}, L_{i,j-1})$, $T_{i,j-1} =_E ck_{i,j-1}$ and $L_{i,j-1} \neq_E nid_{i,j-1}$ since $N_{i,j-1}$ is input by the process and by Lemma 4 $\forall i, k \{^{\mathtt{senc}(T_{h,k},U_{h,k},L_{h,k})}/_{y_{h,k}}\}$ we have that $T_{i,k} = ck_{i,j-1}$ if and only if $h = i, k = j-1$ we have that the message $N_{i,j-1} =_E \mathtt{senc}(ck_{i,j-1}, sr_{i,j-1}, (\text{TMSI\_REALL}, N_{i,j-1}))$ was constructed by the adversary. This is absurd since $ck_{i,j-1}$ is restricted. Hence, $\forall\ i,\ j \in \varphi(D)$ we have that $M_{i,j} = nid_{i,j-1}$.

Let $\sigma^{M_{nid}}_{i,j} = \{^{nid_{i,1}}/_{x_{i,2}}\} \mid \cdots \mid \{^{nid_{i,j-1}}/_{x_{i,j}}\}$ we have that $\forall\ i,\ 1 \le i \le n,\ \varphi(D_i) = \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,j_{nid}}.(\sigma^{M}_{i,j_{id}} \mid \sigma^{K}_{i,j_K} \mid \sigma^{nid}_{i,j_{nid}}) \equiv \nu\, \widetilde{ms}_{i,l_i}.\nu\, \widetilde{nid}_{i,j_{nid}}.(\{^{id_{1,1}}/_{x_{1,1}}\} \mid \sigma^{M_{nid}}_{i,j_{id}} \mid \sigma^{K}_{i,j_K} \mid \sigma^{nid}_{i,j_{nid}})$. Now that we have defined our frame independently from the process input from its memory (or state) we can automatically verify statical equivalence by using the ProVerif tool. We define the following bi-process which outputs the same terms of our process and hence produces the frames $\varphi(C)$ and $\varphi(D)$:

```
free c.
free d.

fun senc/3.
reduc sdec(xk, senc(xk, xr, xm)) = xm.

let S = !new id; new nid; new ck; new sr; new mr;
        out(c, choice[nid, id]) |
        out(d, choice[senc(ck, sr, (tmsi_realloc, nid)), senc(ck, sr, (tmsi_realloc, nid))]) |
        out(c, senc(ck, mr, tmsi_complete)).

process S
```

ProVerif can prove the observational equivalence and consequently the statical equivalence of the two frames. □