A Secure and Regulated Data Access Protocol Proofs

1 Introduction

In what follows, we formally prove that even in case of a scenario with a compromised privileged software, the security of our cryptographic assets is not compromised.

2 Assumptions

We make the following assumptions:

- The *Database* and the *Regulator* are physically separated.
- The direct access to the *Database* outside the protocol, is not possible.
- The adversary has the control of the communication channels and the privileged software like the OS, running on the machines which are running the entities, participating in the protocol.
- The cryptographic assets which include the shared keys among different entities, the service passwords and the initial seed values, are initially distributed and placed inside the enclaves wherever required, in a secure fashion.
- The *Client* is tamper resistant.
- The adversary is *honest but curious*. Thus, the adversary follows the protocol but it can read the messages transferred over the channels and attempt to extract information about the cryptographic assets from those. It can also peek into the memory of the processes running the entities.
- The *Access Control List* is public.
- The encryption and the decryption algorithms are publicly available.
- The algorithms to generate *seeds*, *keys* and *nonces* from a given *seed* value, are publicly available.

3 Predicates and Lemmas

In this section, we introduce the basic lemmas and predicates, which will be extensively used to prove the security invariant as discussed in the above sections.

3.1 Predicates

We introduce a predicate called

$$cKnown(x)$$

.

This predicate is to check if the memory element x is known to the adversary or not. The semantics of the predicate are as follows:

- cKnown(x) : $true$
  If the memory element, x, has gone outside the enclave (in which case it is known to the privileged software) or it can be derived from other memory elements for whom $cKnown(x)$ is true.

- cKnown(x) : $false$
  If the memory element, x, has not gone outside the enclave (in which case it has not been exposed to the privileged software) and it can't be derived from other memory elements for whom $cKnown(x)$ is true.

We also introduce a predicate called

$$mKnown(x)$$

.

This predicate depends on whether the element x has been explicitly made known to the adversary, by moving it out of the enclave. The semantics of this predicate are as follows:

- mKnown(x) : $true$
  If the memory element has been explicitly made known at some point during the protocol execution, i.e, the element has been voluntarily transferred out of the enclave, without any encryption, so that it now becomes known to the adversary

- mKnown(x) : $false$
  If the memory element has not been explicitly made known during the protocol execution until the current point

Next, we go on to introduce the set of lemmas, which will be used in the subsequent sections.

3.2 Lemmas

Using the above predicates, we come up with a few lemmas, based on the properties of the encryption algorithm used and the properties of the SGX enclaves.

1. $$\forall x, mKnown(x) => cKnown(x)$$

2. $$\forall seed, cKnown(seed) => cKnown(NextSeed(seed))$$
   $$\forall seed, cKnown(seed) => cKnown(GenRandomKey(seed))$$
   $$\forall seed, cKnown(seed) => cKnown(GenRandomNonce(seed))$$

3. $$\forall seed,$$
   Given $\neg cKnown(NextSeed(seed))$ until current step, then
   $$\neg cKnown(seed) =>$$
   $$(\neg mKnown(NextSeed(seed)) => \neg cKnown(NextSeed(seed)))$$

4.

$$\forall seed,$$

Given $\neg cKnown(GenRandKey(seed))$ until current step, then

$$\neg cKnown(seed) => $$

$$(\neg mKnown(GenRandKey(seed)) => \neg cKnown(GenRandKey(seed)))$$

5.

$$\forall seed,$$

Given $\neg cKnown(GenRandNonce(seed))$ until current step, then

$$\neg cKnown(seed) => $$

$$(\neg mKnown(GenRandNonce(seed)) => \neg cKnown(GenRandNonce(seed)))$$

6.

$$\forall key, \forall msgSeq,$$

Given $\neg cKnown(key)$ until current step, then

$$cKnown(Enc(key, msgSeq)) => (\neg mKnown(key) => \neg cKnown(key))$$

7.

$$\forall key, \forall msgSeq,$$

Given $\neg cKnown(Enc(key, msgSeq))$ until current step, then

$$\neg cKnown(key) => $$

$$(\neg mKnown(Enc(key, msgSeq)) => \neg cKnown(Enc(key, msgSeq)))$$

8.

$$\forall key, \forall msgSeq,$$

Given $\neg cKnown(msgSeq)$ until current step, then

$$\neg cKnown(key) \wedge cKnown(Enc(key, msgSeq)) => $$

$$(\neg mKnown(msgSeq) => \neg cKnown(msgSeq))$$

9.

$$\forall key, \forall msgSeq,$$

Given $\neg cKnown(key)$ until current step, then

$$\neg cKnown(Enc(key, msgSeq)) => (\neg mKnown(key) => \neg cKnown(key))$$

10.

$$\forall msgSeq, \forall msg,$$

Given $\neg cKnown(msg)$ until current step & $msg \ \epsilon \ msgSeq$, then

$$\neg cKnown(msgSeq) => \neg cKnown(msg)$$

11.

$$\forall msgSeq,$$

$cKnown(msgSeq) => \forall msg \ \epsilon \ msgSeq, cKnown(msg)$

12.

$$\forall x, y, (x = y) => (cKnown(x) <=> cKnown(y))$$

Other than the mentioned lemmas, we make use of *modus ponens* (MP), *modus tollens* (MT) and $\forall$ *elimination* ($\forall E$).

4 Proof

We state and prove the invariant, in this section.

4.1 Invariant

The invariant can be stated as follows:

Given the assumptions as stated in the previous sections, the assets don't get known to the adversary, directly or indirectly, through the channels or the memory of the processes which run the entities taking part in the protocol, over multiple executions of the protocol.

Here, assets refer to:

- The *permanent shared symmetric keys* among the different entities
- The *passwords* of the *ticket granting service* running in the *Regulator* and the *Database service*
- The *session keys* which are generated and shared among the entities, during the protocol execution
- The *query* submitted to the *Database service* by the *client* and its *result*

4.2 Outline of the proof

We prove the invariant stated above, by induction.

$P(n)$ = *The assets don't get known to the adversary, directly or indirectly, through the channels or the memory of the processes which run the entities taking part in the protocol, over 'n' executions of the protocol.*

Basis: For 0 executions of the protocol, the hypothesis reduces to the initial assumption of secure placement of the assets as discussed in the previous sections.

Induction hypothesis: Let $P(k)$ be true.

Induction step: In what follows, we prove that $P(k+1)$ will hold true.

The protocol has been split into multiple *epochs*. We make a forward proof using the *strongest postcondition* approach. At a high level, we begin with the preconditions which hold before the execution of a single epoch, in the protocol. We then derive the strongest postcondition, which holds true after execution of a single statement and using that, we derive the preconditions which hold true before the execution of the next statement. We also use this strongest postcondition to show that the invariant holds after the execution of the current statement and before the execution of the next statement. Repeating this exercise for all the statements in the epoch helps us show that the invariant holds true after the execution of the current epoch as well.

4.3 Proof of the Induction Step

This section contains a subsection for each epoch in the protocol. The subsection contains the preconditions and the statements which are executed in the epoch, along with the proofs of the corresponding invariant.
To ease the proof procedure, we only look at those assets which directly or indirectly get involved, due to the execution of the statement under consideration.

4.3.1 EPOCH Initialiser

Preconditions:

$$\neg cKnown(CK)\ \{Induction\ Hypothesis\}$$

- $m_0 = uname$

$$\dfrac{\dfrac{Lemma\ 1}{\{CK/x\}(Lemma\ 1)}\ \forall E \qquad \neg cKnown(CK)}{\neg mKnown(CK)}\ MT$$

- $Send(Regulator,\ m_0)$

$$\dfrac{\dfrac{\dfrac{Lemma\ 12}{\{m_0/x\}\{uname/y\}(Lemma\ 12)}\ \forall E \qquad m_0 = uname}{cKnown(m_0) <=> cKnown(uname)}\ MP}{cKnown(m_0) => cKnown(uname)}\ Weakening$$

$$\dfrac{\dfrac{Lemma\ 1}{\{m_0/x\}(Lemma\ 1)}\ \forall E \qquad mKnown(m_0)}{cKnown(m_0)}\ MP$$

$$\dfrac{cKnown(m_0) => cKnown(uname) \qquad cKnown(m_0)}{cKnown(uname)}\ MP$$

Postconditions:

$$\neg cKnown(CK)$$

$$cKnown(uname)$$

4.3.2 EPOCH 0

Preconditions:

$$\neg cKnown(k)\ \{Induction\ Hypothesis\}$$

$$\neg cKnown(RK)\ \{Induction\ Hypothesis\}$$

$$\neg cKnown(CK)\ \{Previous\ Epoch\}$$

- $Receive(Client,\ m_0)$

$$cKnown(uname)\ \{Prev\ Epoch\}$$

- $CopyInsideEnclave(m_0)$
- $BeginExecutionInsideEnclave()$
- $unameEnc = Enc(k, [uname])$

$$\dfrac{\dfrac{Lemma\ 7}{\{k/key\}\{[uname]/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(k,[uname]))\ \{vacuity\}}{\neg mKnown(Enc(k,[uname])) => \neg cKnown(Enc(k,[uname]))}\ MP$$

$$\dfrac{\neg mKnown(Enc(k,[uname])) => \neg cKnown(Enc(k,[uname])) \qquad \neg mKnown(Enc(k,[uname]))\ \{Inside\ enclave\}}{\neg cKnown(Enc(k,[uname]))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{k/key\}\{[uname]/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(k)\ \{Precondition\} \qquad \neg cKnown(Enc(k,[uname]))}{\neg mKnown(k) => \neg cKnown(k)}\ MP$$

$$\dfrac{\neg mKnown(k) => \neg cKnown(k) \qquad \neg mKnown(k)\ \{Inside\ enclave\}}{\neg cKnown(k)}\ MP$$

- $clientAuth = Enc(RK, [unameEnc, uname, IPClient])$

$$cKnown(uname)\ \{PrevEpoch\}$$

$$cKnown(IPClient)\ \{Public\}$$

$$Let,\ \ pTxt = [unameEnc, uname, IPClient].\ Then,$$

$$\dfrac{\dfrac{Lemma\ 7}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(RK,pTxt))\ \{vacuity\}}{\neg mKnown(Enc(RK,pTxt)) => \neg cKnown(Enc(RK,pTxt))}\ MP$$

$$\dfrac{\neg mKnown(Enc(RK,pTxt)) => \neg cKnown(Enc(RK,pTxt)) \qquad \neg mKnown(Enc(RK,pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(RK,pTxt))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(RK)\ \{Precondition\} \qquad \neg cKnown(Enc(RK,pTxt))}{\neg mKnown(RK) => \neg cKnown(RK)}\ MP$$

$$\dfrac{\neg mKnown(RK) => \neg cKnown(RK) \qquad \neg mKnown(RK)\ \{Inside\ enclave\}}{\neg cKnown(RK)}\ MP$$

$$Also,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{unameEnc/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{unameEnc/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(unameEnc)}\ MP$$

$$\dfrac{\neg cKnown(unameEnc)}{\neg cKnown(Enc(k,[uname]))}\ \{Enc(k,[uname])/unameEnc\}$$

$$Thus,$$

$$\dfrac{\dfrac{Lemma\ 7}{\{k/key\}\{[uname]/msgSeq\}(Lemma\ 7)}\forall E \qquad \neg cKnown(Enc(k,[uname]))\ \{Prev\ step\}}{\neg mKnown(Enc(k,[uname])) => \neg cKnown(Enc(k,[uname]))}\ MP$$

$$\dfrac{\neg mKnown(Enc(k,[uname])) => \neg cKnown(Enc(k,[uname])) \qquad \neg mKnown(Enc(k,[uname]))\ \{Inside\ enclave\}}{\neg cKnown(Enc(k,[uname]))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{k/key\}\{[uname]/msgSeq\}(Lemma\ 9)}\forall E \qquad \neg cKnown(k)\ \{Precondition\} \qquad \neg cKnown(Enc(k,[uname]))}{\neg mKnown(k) => \neg cKnown(k)}\ MP$$

$$\dfrac{\neg mKnown(k) => \neg cKnown(k) \qquad \neg mKnown(k)\ \{Inside\ enclave\}}{\neg cKnown(k)}\ MP$$

- $m_1 = Enc(CK, [clientAuth])$
- $CopyOutsideEnclave(m_1)$

$$\dfrac{\dfrac{Lemma\ 6}{\{CK/key\}\{[clientAuth]/msgSeq\}(Lemma\ 6)}\forall E \qquad \neg cKnown(CK)\ \{Prev\ Step\} \qquad cKnown(Enc(CK,[clientAuth]))}{\neg mKnown(CK) => \neg cKnown(CK)}\ MP$$

$$\dfrac{\neg mKnown(CK) => \neg cKnown(CK) \qquad \neg mKnown(CK)\ \{Key\ inside\ enclave\}}{\neg cKnown(CK)}\ MP$$

$$\dfrac{\dfrac{Lemma\ 11}{\{clientAuth/msg\}\{[clientAuth]/msgSeq\}(Lemma\ 11)}\forall E \qquad \neg cKnown(clientAuth)\ \{Prev\ step\}}{\neg cKnown([clientAuth])}\ MT$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 8}{\{CK/key\}\{[clientAuth]/msgSeq\}(Lemma\ 8)}\forall E \qquad \neg cKnown(CK)\ \{Proved\} \qquad cKnown(Enc(CK,[clientAuth]))}{\neg mKnown([clientAuth]) => \neg cKnown([clientAuth])}\ MP$$

$$\dfrac{\neg mKnown([clientAuth]) => \neg cKnown([clientAuth]) \qquad \neg mKnown([clientAuth])}{\neg cKnown([clientAuth])}\ MP$$

$$Let,\ pTxt = [unameEnc, uname, IPClient].\ Then,$$

$$\dfrac{\dfrac{\neg cKnown([clientAuth])}{\neg cKnown(clientAuth))}}{\neg cKnown(Enc(RK,pTxt))}\ \{Enc(RK,pTxt)/clientAuth\}$$

$$\dfrac{\dfrac{Lemma\ 7}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\forall E \qquad \neg cKnown(Enc(RK,pTxt))\ \{Proved\}}{\neg mKnown(Enc(RK,pTxt)) => \neg cKnown(Enc(RK,pTxt))}\ MP$$

$$\dfrac{\neg mKnown(Enc(RK,pTxt)) => \neg cKnown(Enc(RK,pTxt)) \qquad \neg mKnown(Enc(RK,pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(RK,pTxt))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(RK)\ \{Precondition\} \qquad \neg cKnown(Enc(RK, pTxt))}{\neg mKnown(RK) => \neg cKnown(RK)}\ MP$$

$$\dfrac{\neg mKnown(RK) => \neg cKnown(RK) \qquad \neg mKnown(RK)\ \{Inside\ enclave\}}{\neg cKnown(RK)}\ MP$$

$$Also,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{unameEnc/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{unameEnc/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(unameEnc)}\ MP$$

$$\dfrac{\neg cKnown(unameEnc)}{\neg cKnown(Enc(k, [uname]))}\ \{Enc(k, [uname])/unameEnc\}$$

$$Thus,$$

$$\dfrac{\dfrac{Lemma\ 7}{\{k/key\}\{[uname]/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(k, [uname]))\ \{Prev\ step\}}{\neg mKnown(Enc(k, [uname])) => \neg cKnown(Enc(k, [uname]))}\ MP$$

$$\dfrac{\neg mKnown(Enc(k, [uname])) => \neg cKnown(Enc(k, [uname])) \qquad \neg mKnown(Enc(k, [uname]))\ \{Inside\ enclave\}}{\neg cKnown(Enc(k, [uname]))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{k/key\}\{[uname]/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(k)\ \{Precondition\} \qquad \neg cKnown(Enc(k, [uname]))}{\neg mKnown(k) => \neg cKnown(k)}\ MP$$

$$\dfrac{\neg mKnown(k) => \neg cKnown(k) \qquad \neg mKnown(k)\ \{Inside\ enclave\}}{\neg cKnown(k)}\ MP$$

- $EndExecutionInsideEnclave()$
- $Send(Client,\ m_1)$

Postconditions:

$$\neg cKnown(CK)$$
$$\neg cKnown(RK)$$
$$\neg cKnown(k)$$
$$cKnown(uname)$$

4.3.3 EPOCH 1

Preconditions:

$$\neg cKnown(SK)\ \{Induction\ Hypothesis\}$$

$$\neg cKnown(CK)\ \{Previous\ Epoch\}$$

$$\neg cKnown(Query)\ \{Assumption\}$$

- $Receive(Regulator,\ m_1)$

$$cKnown(m_1)\ \{Prev\ Epoch\}$$

- $m_1' = Dec(CK, m_1)$

$$m_1' = [clientAuth]$$

- $query = Enc(CK, [Query])$

$$\dfrac{\dfrac{Lemma\ 7}{\{CK/key\}\{[Query]/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(CK,[Query]))\ \{vacuity\}}{\neg mKnown(Enc(CK,[Query])) => \neg cKnown(Enc(CK,[Query]))}\ MP$$

$$\dfrac{\neg mKnown(Enc(CK,[Query])) => \neg cKnown(Enc(CK,[Query])) \qquad \neg mKnown(Enc(CK,[Query]))\ \{Inside\ enclave\}}{\neg cKnown(Enc(CK,[Query]))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{CK/key\}\{[Query]/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(CK)\ \{Precondition\} \qquad \neg cKnown(Enc(CK,[Query]))}{\neg mKnown(CK) => \neg cKnown(CK)}\ MP$$

$$\dfrac{\neg mKnown(CK) => \neg cKnown(CK) \qquad \neg mKnown(CK)\ \{Inside\ enclave\}}{\neg cKnown(CK)}\ MP$$

- $m_2 = Enc(SK, [query, uname, clientAuth])$

$$Let,\ pTxt = [query, uname, clientAuth].\ Then,$$

$$\dfrac{\dfrac{Lemma\ 7}{\{SK/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(SK,pTxt))\ \{vacuity\}}{\neg mKnown(Enc(SK,pTxt)) => \neg cKnown(Enc(SK,pTxt))}\ MP$$

$$\dfrac{\neg mKnown(Enc(SK,pTxt)) => \neg cKnown(Enc(SK,pTxt)) \qquad \neg mKnown(Enc(SK,pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(SK,pTxt))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{SK/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(SK)\ \{Precondition\} \qquad \neg cKnown(Enc(SK,pTxt))}{\neg mKnown(SK) => \neg cKnown(SK)}\ MP$$

$$\dfrac{\neg mKnown(SK) => \neg cKnown(SK) \qquad \neg mKnown(SK)\ \{Inside\ enclave\}}{\neg cKnown(SK)}\ MP$$

$$Also,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(query)}\ MP$$

$$and,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{clientAuth/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(clientAuth)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{clientAuth/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(clientAuth)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(clientAuth)}\ MP$$

$$\dfrac{\neg cKnown(query)}{\neg cKnown(CK)}\ \{Proved\ previously\}$$

$$\dfrac{\neg cKnown(clientAuth)}{\neg cKnown(RK)}\ \{Proved\ previously\}$$

$$\dfrac{\neg cKnown(clientAuth)}{\neg cKnown(k)}\ \{Proved\ previously\}$$

- $Send(Server,\ m_2)$

$$Let,\ pTxt = [query, uname, clientAuth].\ Then,$$

$$\dfrac{\dfrac{\dfrac{Lemma\ 1}{\{m_2/x\}(Lemma\ 1)}\ \forall E \qquad mKnown(m_2)}{cKnown(m_2)}\ MP}{cKnown(Enc(SK, pTxt))}\ \{Enc(SK, pTxt)/m_2\}$$

$$\dfrac{\dfrac{Lemma\ 6}{\{SK/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\ \forall E \qquad \neg cKnown(SK)\ \{Prev\ Step\} \qquad cKnown(Enc(SK, pTxt))}{\neg mKnown(SK) => \neg cKnown(SK)}\ MP$$

$$\dfrac{\neg mKnown(SK) => \neg cKnown(SK) \qquad \neg mKnown(SK)\ \{Key\ inside\ enclave\}}{\neg cKnown(SK)}\ MP$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{clientAuth/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(clientAuth)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 8}{\{SK/key\}\{pTxt/msgSeq\}(Lemma\ 8)}\ \forall E \qquad \neg cKnown(SK)\ \{Proved\} \qquad cKnown(Enc(SK, pTxt))}{\neg mKnown(pTxt) => \neg cKnown(pTxt)}\ MP$$

$$\dfrac{\neg mKnown(pTxt) => \neg cKnown(pTxt) \qquad \neg mKnown(pTxt)}{\neg cKnown(pTxt)}\ MP$$

$$Thus,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(query)}\ MP$$

$$and,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{clientAuth/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(clientAuth)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{clientAuth/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(clientAuth)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(clientAuth)}\ MP$$

$$\dfrac{\neg cKnown(query)}{\neg cKnown(CK)}\ \{Proved\ previously\}$$

$$\dfrac{\neg cKnown(clientAuth)}{\neg cKnown(RK)}\ \{Proved\ previously\}$$

$$\dfrac{\neg cKnown(clientAuth)}{\neg cKnown(k)}\ \{Proved\ previously\}$$

Postconditions:

$$\neg cKnown(SK)$$
$$\neg cKnown(CK)$$
$$\neg cKnown(query)$$
$$\neg cKnown(clientAuth)$$
$$\neg cKnown(RK)$$
$$\neg cKnown(k)$$
$$cKnown(uname)$$

4.3.4 EPOCH 2

Preconditions:

$$\neg cKnown(SK)\ \{Previous\ Epoch\}$$

$$\neg cKnown(RK)\ \{Previous\ Epoch\}$$

$$\neg cKnown(query)\ \{Previous\ Epoch\}$$

$$\neg cKnown(clientAuth)\ \{Previous\ Epoch\}$$

$$\neg cKnown(unameEnc)\ \{Previous\ Epoch\}$$

- $Receive(Client,\ m_2)$

$$cKnown(m_2)\ \{Prev\ Epoch\}$$

- $CopyInsideEnclave(m_2)$
- $BeginExecutionInsideEnclave()$
- $m_2' = Dec(SK, m_2)$

$$m_2' = [query, uname, clientAuth]$$

$$Let,\ pTxt = [query, uname, clientAuth].\ Then,$$

$$\frac{\neg cKnown(query) \qquad \neg cKnown(clientAuth)}{\neg cKnown(pTxt)}\ \{Lemma\ 11\}$$

$$Thus,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(query)}\ MP$$

$$and,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{clientAuth/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(clientAuth)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{clientAuth/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(clientAuth)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(clientAuth)}\ MP$$

- $clientAuth' = Dec(RK, clientAuth)$

$$clientAuth' = [unameEnc, uname, IPClient]$$

$$Let,\ pTxt = [unameEnc, uname, IPClient].\ Then,$$

$$\frac{\neg cKnown(unameEnc)}{\neg cKnown(pTxt)}\ \{Lemma\ 11\}$$

$$Thus,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{unameEnc/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{unameEnc/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(unameEnc)}\ MP$$

- $Checks\ for\ equality\ of\ uname\ and\ IPClient\ across\ epochs$
- $m_3 = Enc(RK, clientAuth')$

$$Let,\ cAuth' = clientAuth'.\ Then,$$

$$\cfrac{\cfrac{Lemma\ 7}{\{RK/key\}\{cAuth'/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(RK, cAuth'))\ \{vacuity\}}{\neg mKnown(Enc(RK, cAuth')) => \neg cKnown(Enc(RK, cAuth'))}\ MP$$

$$\cfrac{\neg mKnown(Enc(RK, cAuth')) => \neg cKnown(Enc(RK, cAuth')) \qquad \neg mKnown(Enc(RK, cAuth'))\ \{Inside\ enclave\}}{\neg cKnown(Enc(RK, cAuth'))}\ MP$$

$$\cfrac{\cfrac{Lemma\ 9}{\{RK/key\}\{cAuth'/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(RK)\ \{Precondition\} \qquad \neg cKnown(Enc(RK, cAuth'))}{\neg mKnown(RK) => \neg cKnown(RK)}\ MP$$

$$\cfrac{\neg mKnown(RK) => \neg cKnown(RK) \qquad \neg mKnown(RK)\ \{Inside\ enclave\}}{\neg cKnown(RK)}\ MP$$

$$Now,$$

$$\neg cKnown(unameEnc)\ \{Prev\ Step\}$$

$$Thus,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{unameEnc/msg\}\{cAuth'/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\}}{\neg cKnown(cAuth')}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{unameEnc/msg\}\{cAuth'/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\} \qquad \neg cKnown(cAuth')}{\neg cKnown(unameEnc)}\ MP$$

$$\frac{\neg cKnown(unameEnc)}{\neg cKnown(k)}\ \{Proved\ Before\}$$

- $CopyOutsideEnclave(m_3)$

$$\dfrac{\dfrac{Lemma\ 6}{\{RK/key\}\{clientAuth'/msgSeq\}(Lemma\ 6)}\forall E \qquad \neg cKnown(RK)\ \{Prev\ Step\} \qquad cKnown(Enc(RK, clientAuth'))}{\neg mKnown(RK) => \neg cKnown(RK)}\ MP$$

$$\dfrac{\neg mKnown(RK) => \neg cKnown(RK) \qquad \neg mKnown(RK)\ \{Key\ inside\ enclave\}}{\neg cKnown(RK)}\ MP$$

$$At\ the\ previous\ step,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{unameEnc/msg\}\{clientAuth'/msgSeq\}(Lemma\ 11)}\forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\}}{\neg cKnown(clientAuth')}\ MT$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 8}{\{RK/key\}\{clientAuth'/msgSeq\}(Lemma\ 8)}\forall E \qquad \neg cKnown(RK)\ \{Proved\} \qquad cKnown(Enc(RK, clientAuth'))}{\neg mKnown(clientAuth') => \neg cKnown(clientAuth')}\ MP$$

$$\dfrac{\neg mKnown(clientAuth') => \neg cKnown(clientAuth') \qquad \neg mKnown(clientAuth')}{\neg cKnown(clientAuth')}\ MP$$

$$Thus,$$

$$\dfrac{\neg cKnown(unameEnc)}{\neg cKnown(Enc(k, [uname]))}\ \{Enc(k, [uname])/unameEnc\}$$

$$Thus,$$

$$\dfrac{\dfrac{Lemma\ 7}{\{k/key\}\{[uname]/msgSeq\}(Lemma\ 7)}\forall E \qquad \neg cKnown(Enc(k, [uname]))\ \{Prev\ step\}}{\neg mKnown(Enc(k, [uname])) => \neg cKnown(Enc(k, [uname]))}\ MP$$

$$\dfrac{\neg mKnown(Enc(k, [uname])) => \neg cKnown(Enc(k, [uname])) \qquad \neg mKnown(Enc(k, [uname]))\ \{Inside\ enclave\}}{\neg cKnown(Enc(k, [uname]))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{k/key\}\{[uname]/msgSeq\}(Lemma\ 9)}\forall E \qquad \neg cKnown(k)\ \{Precondition\} \qquad \neg cKnown(Enc(k, [uname]))}{\neg mKnown(k) => \neg cKnown(k)}\ MP$$

$$\dfrac{\neg mKnown(k) => \neg cKnown(k) \qquad \neg mKnown(k)\ \{Inside\ enclave\}}{\neg cKnown(k)}\ MP$$

- $EndExecutionInsideEnclave()$
- $Send(Client,\ m_3)$

Postconditions:

$$\neg cKnown(SK)$$
$$\neg cKnown(query)$$
$$\neg cKnown(RK)$$
$$\neg cKnown(k)$$
$$\neg cKnown(unameEnc)$$
$$\neg cKnown(clientAuth)$$
$$cKnown(uname)$$

4.3.5 EPOCH 3

Preconditions:

$$\neg cKnown(k)\ \{Previous\ Epoch\}$$
$$\neg cKnown(RK)\ \{Previous\ Epoch\}$$
$$\neg cKnown(TGS_{Passwd})\ \{InductionHypothesis\}$$
$$\neg cKnown(Seed_{Reg})\ \{InductionHypothesis\}$$

- $Receive(Server,\ m_3)$

$$cKnown(m_3)\ \{Prev\ Epoch\}$$

- $CopyInsideEnclave(m_3)$
- $BeginExecutionInsideEnclave()$
- $m_3' = Dec(RK, m_3)$

$$m_3' = [unameEnc, uname, IPClient]$$

$$\cfrac{\cfrac{Lemma\ 11}{\{unameEnc/msg\}\{m_3'/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\}}{\neg cKnown(m_3')}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{unameEnc/msg\}\{m_3'/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(unameEnc)\ \{Prev\ step\} \qquad \neg cKnown(m_3')}{\neg cKnown(unameEnc)}\ MP$$

$$Thus,$$

$$\cfrac{\neg cKnown(unameEnc)}{\neg cKnown(k)}\ Proved\ before$$

- $uname_1 = Dec(k, unameEnc)$

$$uname_1 = uname$$

$$\neg cKnown(k)\ \{Execution\ inside\ enclave\}$$

- $Checks\ for\ equality\ of\ uname\ and\ IPClient\ across\ epochs$
- $SK_{TGS} = GenRandomKey(Seed_{Reg})$

$$Let,\ sd = Seed_{Reg}$$

$$\dfrac{\dfrac{Lemma\ 4}{\{sd/seed\}(Lemma\ 4)}\ \forall E \qquad \neg cKnown(GenRandomKey(sd))\ \{vacuity\} \qquad \neg cKnown(sd)\ \{vacuity\}}{\neg mKnown(GenRandomKey(sd)) => \neg cKnown(GenRandomKey(sd))}\ MP$$

$$Then,$$

$$\dfrac{\neg mKnown(GenRandomKey(sd)) => \neg cKnown(GenRandomKey(sd)) \qquad \neg mKnown(GenRandomKey(sd))}{\neg cKnown(GenRandomKey(sd))}\ MP$$

- $Seed_{Reg} = NextSeed(Seed_{Reg})$

$$Let,\ sd = Seed_{Reg}$$

$$\dfrac{\dfrac{Lemma\ 3}{\{sd/seed\}(Lemma\ 3)}\ \forall E \qquad \neg cKnown(NextSeed(sd))\ \{vacuity\} \qquad \neg cKnown(sd)\ \{vacuity\}}{\neg mKnown(NextSeed(sd)) => \neg cKnown(NextSeed(sd))}\ MP$$

$$Then,$$

$$\dfrac{\neg mKnown(NextSeed(sd)) => \neg cKnown(NextSeed(sd)) \qquad \neg mKnown(NextSeed(sd))}{\neg cKnown(NextSeed(sd))}\ MP$$

- $TGT_{List} = [uname, IPServer, timestamp, lifespan, SK_{TGS}]$

$$cKnown(uname)$$

$$cKnown(IPServer)$$

$$cKnown(timestamp)$$

$$cKnown(lifespan)$$

$$\dfrac{\dfrac{Lemma\ 11}{\{SK_{TGS}/msg\}\{TGT_{List}/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\}}{\neg cKnown(TGT_{List})}\ MT$$

- $TGT = Enc(TGS_{Passwd}, TGT_{List})$

$$Let,\ TGS_P = TGS_{Passwd}\ and\ pTxt = TGT_{List}.\ Then,$$

$$\dfrac{\dfrac{Lemma\ 7}{\{TGS_P/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(TGS_P, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(TGS_P, pTxt)) => \neg cKnown(Enc(TGS_P, pTxt))}\ MP$$

$$\dfrac{\neg mKnown(Enc(TGS_P, pTxt)) => \neg cKnown(Enc(TGS_P, pTxt)) \qquad \neg mKnown(Enc(TGS_P, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(TGS_P, pTxt))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{TGS_P/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(TGS_P)\ \{Precondition\} \qquad \neg cKnown(Enc(TGS_P, pTxt))}{\neg mKnown(TGS_P) => \neg cKnown(TGS_P)}\ MP$$

$$\dfrac{\neg mKnown(TGS_P) => \neg cKnown(TGS_P) \qquad \neg mKnown(TGS_P)\ \{Inside\ enclave\}}{\neg cKnown(TGS_P)}\ MP$$

- $m_4 = Enc(RK, [SK_{TGS}, TGT])$

$$Let,\ pTxt = [SK_{TGS}, TGT].\ Then,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{SK_{TGS}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Also,$$

$$\dfrac{\dfrac{Lemma\ 7}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(RK, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(RK, pTxt)) => \neg cKnown(Enc(RK, pTxt))}\ MP$$

$$\dfrac{\neg mKnown(Enc(RK, pTxt)) => \neg cKnown(Enc(RK, pTxt)) \qquad \neg mKnown(Enc(RK, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(RK, pTxt))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(RK)\ \{Precondition\} \qquad \neg cKnown(Enc(RK, pTxt))}{\neg mKnown(RK) => \neg cKnown(RK)}\ MP$$

$$\dfrac{\neg mKnown(RK) => \neg cKnown(RK) \qquad \neg mKnown(RK)\ \{Inside\ enclave\}}{\neg cKnown(RK)}\ MP$$

- $CopyOutsideEnclave(m_4)$

$$Let,\ pTxt = [SK_{TGS}, TGT].\ Then,$$

$$\dfrac{\dfrac{Lemma\ 6}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\ \forall E \qquad \neg cKnown(RK)\ \{Prev\ Step\} \qquad cKnown(Enc(RK, pTxt))}{\neg mKnown(RK) => \neg cKnown(RK)}\ MP$$

$$\dfrac{\neg mKnown(RK) => \neg cKnown(RK) \qquad \neg mKnown(RK)\ \{Key\ inside\ enclave\}}{\neg cKnown(RK)}\ MP$$

$$At\ the\ previous\ step,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{SK_{TGS}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 8}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 8)}\ \forall E \qquad \neg cKnown(RK)\ \{Proved\} \qquad cKnown(Enc(RK, pTxt))}{\neg mKnown(pTxt) => \neg cKnown(pTxt)}\ MP$$

$$\frac{\neg mKnown(pTxt) => \neg cKnown(pTxt) \qquad \neg mKnown(pTxt)}{\neg cKnown(pTxt)} MP$$

$$Thus,$$

$$\frac{\dfrac{Lemma\ 11}{\{SK_{TGS}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)} \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\}}{\neg cKnown(pTxt)} MT$$

$$\frac{\dfrac{Lemma\ 10}{\{SK_{TGS}/msg\}\{pTxt/msgSeq\}(Lemma\ 10)} \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(SK_{TGS})} MP$$

- $EndExecutionInsideEnclave()$
- $Send(Client,\ m_4)$

Postconditions:

$$\neg cKnown(SK_{TGS})$$
$$\neg cKnown(RK)$$
$$\neg cKnown(k)$$
$$\neg cKnown(TGS_{Passwd})$$
$$\neg cKnown(Seed_{Reg})$$

4.3.6 EPOCH 4

Preconditions:

$$\neg cKnown(RK)\ \{Previous\ Epoch\}$$
$$\neg cKnown(SK_{TGS})\ \{Previous\ Epoch\}$$
$$\neg cKnown(query)\ \{Previous\ Epoch\}$$

- $Receive(Regulator,\ m_4)$

$$cKnown(m_4)\ \{Prev\ Epoch\}$$

- $CopyInsideEnclave(m_4)$
- $BeginExecutionInsideEnclave()$
- $m'_4 = Dec(RK, m_4)$

$$m'_4 = [SK_{TGS}, TGT]$$

$$\frac{\dfrac{Lemma\ 11}{\{SK_{TGS}/msg\}\{m'_4/msgSeq\}(Lemma\ 11)} \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\}}{\neg cKnown(m'_4)} MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{SK_{TGS}/msg\}\{m_4'/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\} \qquad \neg cKnown(m_4')}{\neg cKnown(SK_{TGS})}\ MP$$

- $Auth = Enc(SK_{TGS}, [uname, IPServer])$

$$Let,\ pTxt = [uname, IPServer]\ and\ sk = SK_{TGS}.\ Then,$$

$$\dfrac{cKnown(uname) \qquad cKnown(IPServer)}{cKnown(pTxt)}\ All\ Components\ Known$$

$$\dfrac{\dfrac{Lemma\ 7}{\{sk/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(sk, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(sk, pTxt)) => \neg cKnown(Enc(sk, pTxt))}\ MP$$

$$\dfrac{\neg mKnown(Enc(sk, pTxt)) => \neg cKnown(Enc(sk, pTxt)) \qquad \neg mKnown(Enc(sk, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(sk, pTxt))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{sk/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(sk)\ \{Precondition\} \qquad \neg cKnown(Enc(sk, pTxt))}{\neg mKnown(sk) => \neg cKnown(sk)}\ MP$$

$$\dfrac{\neg mKnown(sk) => \neg cKnown(sk) \qquad \neg mKnown(sk)\ \{Inside\ enclave\}}{\neg cKnown(sk)}\ MP$$

- $m_5 = Enc(SK_{TGS}, [query, TGT, Auth])$

$$Let,\ pTxt = [query, TGT, Auth].\ Then,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\neg cKnown(Auth) \qquad \neg cKnown(pTxt)}{\neg cKnown(Auth)}\ MP$$

$$\dfrac{\neg cKnown(query) \qquad \neg cKnown(pTxt)}{\neg cKnown(query)}\ MP$$

$$Also,$$

$$\dfrac{\dfrac{Lemma\ 7}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(RK, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(RK, pTxt)) => \neg cKnown(Enc(RK, pTxt))}\ MP$$

$$\dfrac{\neg mKnown(Enc(RK, pTxt)) => \neg cKnown(Enc(RK, pTxt)) \qquad \neg mKnown(Enc(RK, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(RK, pTxt))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{RK/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(RK)\ \{Precondition\} \qquad \neg cKnown(Enc(RK, pTxt))}{\neg mKnown(RK) => \neg cKnown(RK)}\ MP$$

$$\frac{\neg mKnown(RK) => \neg cKnown(RK) \qquad \neg mKnown(RK)\ \{Inside\ enclave\}}{\neg cKnown(RK)}\ MP$$

- $CopyOutsideEnclave(m_5)$

$$Let,\ pTxt = [query, TGT, Auth].\ Then,$$

$$\frac{\dfrac{Lemma\ 6}{\{SK_{TGS}/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ Step\} \qquad cKnown(Enc(SK_{TGS}, pTxt))}{\neg mKnown(SK_{TGS}) => \neg cKnown(SK_{TGS})}\ MP$$

$$\frac{\neg mKnown(SK_{TGS}) => \neg cKnown(SK_{TGS}) \qquad \neg mKnown(SK_{TGS})\ \{Key\ inside\ enclave\}}{\neg cKnown(SK_{TGS})}\ MP$$

$$At\ the\ previous\ step,$$

$$\frac{\dfrac{Lemma\ 11}{\{SK_{TGS}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Then,$$

$$\frac{\dfrac{Lemma\ 8}{\{SK_{TGS}/key\}\{pTxt/msgSeq\}(Lemma\ 8)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Proved\} \qquad cKnown(Enc(SK_{TGS}, pTxt))}{\neg mKnown(pTxt) => \neg cKnown(pTxt)}\ MP$$

$$\frac{\neg mKnown(pTxt) => \neg cKnown(pTxt) \qquad \neg mKnown(pTxt)}{\neg cKnown(pTxt)}\ MP$$

$$Thus,$$

$$\frac{\dfrac{Lemma\ 11}{\{SK_{TGS}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\frac{\dfrac{Lemma\ 10}{\{SK_{TGS}/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(SK_{TGS})}\ MP$$

- $EndExecutionInsideEnclave()$
- $Send(Regulator,\ m_5)$

Postconditions:

$$\neg cKnown(SK_{TGS})$$

$$\neg cKnown(RK)$$

$$\neg cKnown(k)$$

$$\neg cKnown(query)$$

4.3.7 EPOCH 5

Preconditions:

$$\neg cKnown(cKey)\ \{Induction\ Hypothesis\}$$

$$\neg cKnown(Svc_{Passwd})\ \{Induction\ Hypothesis\}$$

$$\neg cKnown(SK_{TGS})\ \{Previous\ Epoch\}$$

$$\neg cKnown(TGS_{Passwd})\ \{Previous\ Epoch\}$$

$$\neg cKnown(Seed_{Reg})\ \{Previous\ Epoch\}$$

$$\neg cKnown(query)\ \{Previous\ Epoch\}$$

- $Receive(Server,\ m_5)$

$$cKnown(m_5)\ \{Prev\ Epoch\}$$

- $CopyInsideEnclave(m_5)$
- $BeginExecutionInsideEnclave()$
- $m_5' = Dec(SK_{TGS}, m_5)$

$$m_5' = [query, TGT, Auth]$$

$$\dfrac{\dfrac{Lemma\ 11}{\{query/msg\}\{m_5'/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(m_5')}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{query/msg\}\{m_5'/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\} \qquad \neg cKnown(m_5')}{\neg cKnown(query)}\ MP$$

$$Also,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{Auth/msg\}\{m_5'/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(Auth)\ \{Prev\ step\}}{\neg cKnown(m_5')}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{Auth/msg\}\{m_5'/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(Auth)\ \{Prev\ step\} \qquad \neg cKnown(m_5')}{\neg cKnown(Auth)}\ MP$$

$$Thus,$$

$$\dfrac{\neg cKnown(query)}{\neg cKnown(CK)}\ Proved\ before$$

$$\dfrac{\neg cKnown(Auth)}{\neg cKnown(SK_{TGS})}\ Proved\ before$$

- $DecTGT = Dec(TGS_{Passwd}, TGT)$

$$DecTGT = [uname, IPServer, timestamp, lifespan, SK_{TGS}]$$

$$\cfrac{\cfrac{Lemma\ 11}{\{SK_{TGS}/msg\}\{DecTGT/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\}}{\neg cKnown(DecTGT)}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{SK_{TGS}/msg\}\{DecTGT/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ step\} \qquad \neg cKnown(DecTGT)}{\neg cKnown(SK_{TGS})}\ MP$$

$$Also,$$

$$\neg cKnown(TGS_{Passwd})\ \{Inside\ Enclave\ \&\ Previous\ Epoch\}$$

- $DecAuth = Dec(SK_{TGS}, Auth)$

$$DecAuth = [uname, IPServer]$$

$$\cfrac{cKnown(uname) \qquad cKnown(IPServer)}{cKnown(DecAuth)}\ All\ Components\ Known$$

$$Also,$$

$$\neg cKnown(SK_{TGS})\ \{Inside\ Enclave\}$$

- $Validation\ for\ uname\ and\ IPServer$
- $Validation\ for\ timestamp\ and\ lifespan$
- $Authorisation\ using\ Access\ Control\ List$
- $DecQuery = Dec(cKey, query)$

$$cKey = CK$$

$$DecQuery = [Query]$$

$$\neg cKnown(Query)\ \{Previous\ Epoch\}$$

$$\neg cKnown(cKey)\ \{Previous\ Epoch\ \&\ Inside\ Enclave\}$$

- $SK_{Svc} = GenRandomKey(Seed_{Reg})$

$$Let,\ sd = Seed_{Reg}$$

$$\cfrac{\cfrac{Lemma\ 4}{\{sd/seed\}(Lemma\ 4)}\ \forall E \qquad \neg cKnown(GenRandomKey(sd))\ \{vacuity\} \qquad \neg cKnown(sd)\ \{vacuity\}}{\neg mKnown(GenRandomKey(sd)) => \neg cKnown(GenRandomKey(sd))}\ MP$$

$$Then,$$

$$\frac{\neg mKnown(GenRandomKey(sd)) => \neg cKnown(GenRandomKey(sd)) \qquad \neg mKnown(GenRandomKey(sd))}{\neg cKnown(GenRandomKey(sd))}\ MP$$

- $Seed_{Reg} = NextSeed(Seed_{Reg})$

$$Let,\ sd = Seed_{Reg}$$

$$\frac{\dfrac{Lemma\ 3}{\{sd/seed\}(Lemma\ 3)}\ \forall E \qquad \neg cKnown(NextSeed(sd))\ \{vacuity\} \qquad \neg cKnown(sd)\ \{vacuity\}}{\neg mKnown(NextSeed(sd)) => \neg cKnown(NextSeed(sd))}\ MP$$

$$Then,$$

$$\frac{\neg mKnown(NextSeed(sd)) => \neg cKnown(NextSeed(sd)) \qquad \neg mKnown(NextSeed(sd))}{\neg cKnown(NextSeed(sd))}\ MP$$

- $SvcTkt_{List} = [uname, IPServer, timestamp, lifespan, SK_{Svc}, cKey, query]$

$$cKnown(uname)$$

$$cKnown(IPServer)$$

$$cKnown(timestamp)$$

$$cKnown(lifespan)$$

$$\neg cKnown(cKey)$$

$$\neg cKnown(query)$$

$$\frac{\dfrac{Lemma\ 11}{\{SK_{Svc}/msg\}\{SvcTkt_{List}/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\}}{\neg cKnown(SvcTkt_{List})}\ MT$$

- $SvcTkt = Enc(Svc_{Passwd}, SvcTkt_{List})$

$$Let,\ Svc_P = Svc_{Passwd}\ and\ pTxt = SvcTkt_{List}.\ Then,$$

$$\frac{\dfrac{Lemma\ 7}{\{Svc_P/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(Svc_P, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(Svc_P, pTxt)) => \neg cKnown(Enc(Svc_P, pTxt))}\ MP$$

$$\frac{\neg mKnown(Enc(Svc_P, pTxt)) => \neg cKnown(Enc(Svc_P, pTxt)) \qquad \neg mKnown(Enc(Svc_P, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(Svc_P, pTxt))}\ MP$$

$$\frac{\dfrac{Lemma\ 9}{\{Svc_P/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(Svc_P)\ \{Precondition\} \qquad \neg cKnown(Enc(Svc_P, pTxt))}{\neg mKnown(Svc_P) => \neg cKnown(Svc_P)}\ MP$$

$$\frac{\neg mKnown(Svc_P) => \neg cKnown(Svc_P) \qquad \neg mKnown(Svc_P)\ \{Inside\ enclave\}}{\neg cKnown(Svc_P)}\ MP$$

- $m_6 = Enc(SK_{TGS}, [SK_{Svc}, SvcTkt])$

$$Let,\ pTxt = [SK_{Svc}, SvcTkt].\ Then,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{SK_{Svc}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Also,$$

$$\cfrac{\cfrac{Lemma\ 7}{\{SK_{TGS}/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(SK_{TGS}, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(SK_{TGS}, pTxt)) => \neg cKnown(Enc(SK_{TGS}, pTxt))}\ MP$$

$$\cfrac{\neg mKnown(Enc(SK_{TGS}, pTxt)) => \neg cKnown(Enc(SK_{TGS}, pTxt)) \qquad \neg mKnown(Enc(SK_{TGS}, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(SK_{TGS}, pTxt))}\ MP$$

$$\cfrac{\cfrac{Lemma\ 9}{\{SK_{TGS}/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Precondition\} \qquad \neg cKnown(Enc(SK_{TGS}, pTxt))}{\neg mKnown(SK_{TGS}) => \neg cKnown(SK_{TGS})}\ MP$$

$$\cfrac{\neg mKnown(SK_{TGS}) => \neg cKnown(SK_{TGS}) \qquad \neg mKnown(SK_{TGS})\ \{Inside\ enclave\}}{\neg cKnown(SK_{TGS})}\ MP$$

- $CopyOutsideEnclave(m_6)$

$$Let,\ pTxt = [SK_{Svc}, SvcTkt].\ Then,$$

$$\cfrac{\cfrac{Lemma\ 6}{\{SK_{TGS}/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Prev\ Step\} \qquad cKnown(Enc(SK_{TGS}, pTxt))}{\neg mKnown(SK_{TGS}) => \neg cKnown(SK_{TGS})}\ MP$$

$$\cfrac{\neg mKnown(SK_{TGS}) => \neg cKnown(SK_{TGS}) \qquad \neg mKnown(SK_{TGS})\ \{Key\ inside\ enclave\}}{\neg cKnown(SK_{TGS})}\ MP$$

$$At\ the\ previous\ step,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{SK_{Svc}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Then,$$

$$\cfrac{\cfrac{Lemma\ 8}{\{SK_{TGS}/key\}\{pTxt/msgSeq\}(Lemma\ 8)}\ \forall E \qquad \neg cKnown(SK_{TGS})\ \{Proved\} \qquad cKnown(Enc(SK_{TGS}, pTxt))}{\neg mKnown(pTxt) => \neg cKnown(pTxt)}\ MP$$

$$\cfrac{\neg mKnown(pTxt) => \neg cKnown(pTxt) \qquad \neg mKnown(pTxt)}{\neg cKnown(pTxt)}\ MP$$

$$Thus,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{SK_{Svc}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{SK_{Svc}/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(SK_{Svc})}\ MP$$

- $EndExecutionInsideEnclave()$
- $Send(Server,\ m_6)$

Postconditions:

$$\neg cKnown(cKey)$$
$$\neg cKnown(SK_{TGS})$$
$$\neg cKnown(TGS_{Passwd})$$
$$\neg cKnown(Svc_{Passwd})$$
$$\neg cKnown(Seed_{Reg})$$
$$\neg cKnown(SK_{Svc})$$
$$\neg cKnown(query)$$

4.3.8 EPOCH 6

Preconditions:

$$\neg cKnown(Seed_{Server})\ \{Induction\ Hypothesis\}$$
$$\neg cKnown(cKey)\ \{Previous\ Epoch\}$$
$$\neg cKnown(SK_{TGS})\ \{Previous\ Epoch\}$$
$$\neg cKnown(SK_{Svc})\ \{Previous\ Epoch\}$$
$$\neg cKnown(SvcTkt)\ \{Previous\ Epoch\}$$

- $Receive(Regulator,\ m_6)$

$$cKnown(m_6)\ \{Prev\ Epoch\}$$

- $CopyInsideEnclave(m_6)$
- $BeginExecutionInsideEnclave()$
- $m_6' = Dec(SK_{TGS}, m_6)$

$$m_6' = [SK_{Svc}, SvcTkt]$$

$$\dfrac{\dfrac{Lemma\ 11}{\{Sk_{Svc}/msg\}\{m_6'/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(Sk_{Svc})\ \{Prev\ step\}}{\neg cKnown(m_6')}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{Sk_{Svc}/msg\}\{m_6'/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(Sk_{Svc})\ \{Prev\ step\} \qquad \neg cKnown(m_6')}{\neg cKnown(Sk_{Svc})}\ MP$$

$$Also,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{SvcTkt/msg\}\{m_6'/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SvcTkt)\ \{Prev\ step\}}{\neg cKnown(m_6')}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{SvcTkt/msg\}\{m_6'/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(SvcTkt)\ \{Prev\ step\} \qquad \neg cKnown(m_6')}{\neg cKnown(SvcTkt)}\ MP$$

$$\dfrac{\neg cKnown(Auth)}{\neg cKnown(SK_{TGS})}\ Proved\ before$$

- $Auth = Enc(SK_{Svc}, [uname, IPServer])$

$$Let,\ pTxt = [uname, IPServer]\ and\ sk = SK_{Svc}.\ Then,$$

$$\dfrac{cKnown(uname) \qquad cKnown(IPServer)}{cKnown(pTxt)}\ All\ Components\ Known$$

$$\dfrac{\dfrac{Lemma\ 7}{\{sk/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(sk, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(sk, pTxt)) => \neg cKnown(Enc(sk, pTxt))}\ MP$$

$$\dfrac{\neg mKnown(Enc(sk, pTxt)) => \neg cKnown(Enc(sk, pTxt)) \qquad \neg mKnown(Enc(sk, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(sk, pTxt))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{sk/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(sk)\ \{Precondition\} \qquad \neg cKnown(Enc(sk, pTxt))}{\neg mKnown(sk) => \neg cKnown(sk)}\ MP$$

$$\dfrac{\neg mKnown(sk) => \neg cKnown(sk) \qquad \neg mKnown(sk)\ \{Inside\ enclave\}}{\neg cKnown(sk)}\ MP$$

- $nonce = GenRandomNonce(Seed_{Server})$

$$Let,\ sd = Seed_{Server}$$

$$\dfrac{\dfrac{Lemma\ 4}{\{sd/seed\}(Lemma\ 4)}\ \forall E \qquad \neg cKnown(GenRandomNonce(sd))\ \{vacuity\} \qquad \neg cKnown(sd)\ \{vacuity\}}{\neg mKnown(GenRandomNonce(sd)) => \neg cKnown(GenRandomNonce(sd))}\ MP$$

$$Then,$$

$$\dfrac{\neg mKnown(GenRandomNonce(sd)) => \neg cKnown(GenRandomNonce(sd)) \qquad \neg mKnown(GenRandomNonce(sd))}{\neg cKnown(GenRandomNonce(sd))}\ MP$$

- $Seed_{Reg} = NextSeed(Seed_{Server})$

$$Let,\ sd = Seed_{Server}$$

$$\cfrac{\cfrac{Lemma\ 3}{\{sd/seed\}(Lemma\ 3)}\forall E \qquad \neg cKnown(NextSeed(sd))\ \{vacuity\} \qquad \neg cKnown(sd)\ \{vacuity\}}{\neg mKnown(NextSeed(sd)) => \neg cKnown(NextSeed(sd))}\ MP$$

$$Then,$$

$$\cfrac{\neg mKnown(NextSeed(sd)) => \neg cKnown(NextSeed(sd)) \qquad \neg mKnown(NextSeed(sd))}{\neg cKnown(NextSeed(sd))}\ MP$$

- $Nonce = Enc(SK_{Svc}, [nonce])$

$$Let,\ sk = SK_{Svc}.\ Then,$$

$$\cfrac{\cfrac{Lemma\ 7}{\{sk/key\}\{[nonce]/msgSeq\}(Lemma\ 7)}\forall E \qquad \neg cKnown(Enc(sk, [nonce]))\ \{vacuity\}}{\neg mKnown(Enc(sk, [nonce])) => \neg cKnown(Enc(sk, [nonce]))}\ MP$$

$$\cfrac{\neg mKnown(Enc(sk, [nonce])) => \neg cKnown(Enc(sk, [nonce])) \qquad \neg mKnown(Enc(sk, [nonce]))\ \{Inside\ enclave\}}{\neg cKnown(Enc(sk, [nonce]))}\ MP$$

$$\cfrac{\cfrac{Lemma\ 9}{\{sk/key\}\{[nonce]/msgSeq\}(Lemma\ 9)}\forall E \qquad \neg cKnown(sk)\ \{Precondition\} \qquad \neg cKnown(Enc(sk, [nonce]))}{\neg mKnown(sk) => \neg cKnown(sk)}\ MP$$

$$\cfrac{\neg mKnown(sk) => \neg cKnown(sk) \qquad \neg mKnown(sk)\ \{Inside\ enclave\}}{\neg cKnown(sk)}\ MP$$

- $m_7 = [SvcTkt, Auth, Nonce]$
- $CopyOutsideEnclave(m_7)$

$$Let,\ sp = Svc_{Passwd}\ and\ pTxt = SvcTkt_{List}.\ Then,$$

$$\cfrac{\cfrac{Lemma\ 6}{\{sp/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\forall E \qquad \neg cKnown(sp)\ \{Prev\ Step\} \qquad cKnown(Enc(sp, pTxt))}{\neg mKnown(sp) => \neg cKnown(sp)}\ MP$$

$$\cfrac{\neg mKnown(sp) => \neg cKnown(sp) \qquad \neg mKnown(sp)\ \{Key\ inside\ enclave\}}{\neg cKnown(sp)}\ MP$$

$$At\ the\ previous\ step,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{SK_{Svc}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Then,$$

$$\cfrac{\cfrac{Lemma\ 8}{\{sp/key\}\{pTxt/msgSeq\}(Lemma\ 8)}\forall E \qquad \neg cKnown(sp)\ \{Proved\} \qquad cKnown(Enc(sp, pTxt))}{\neg mKnown(pTxt) => \neg cKnown(pTxt)}\ MP$$

$$\frac{\neg mKnown(pTxt) => \neg cKnown(pTxt) \qquad \neg mKnown(pTxt)}{\neg cKnown(pTxt)}\ MP$$

$$Thus,$$

$$\frac{\dfrac{Lemma\ 11}{\{SK_{Svc}/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\frac{\dfrac{Lemma\ 10}{\{SK_{Svc}/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(SK_{Svc})}\ MP$$

$$Also,$$

$$\neg cKnown(cKey)\ \{Precondition\}$$

$$\frac{\dfrac{Lemma\ 11}{\{cKey/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(cKey)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\frac{\dfrac{Lemma\ 10}{\{cKey/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(cKey)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(cKey)}\ MP$$

$$Now,$$
$$Let,\ sk = SK_{Svc}\ and\ pTxt = [uname, IPServer].\ Then,$$

$$\frac{\dfrac{Lemma\ 6}{\{sk/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\ \forall E \qquad \neg cKnown(sk)\ \{Prev\ Step\} \qquad cKnown(Enc(sk, pTxt))}{\neg mKnown(sk) => \neg cKnown(sk)}\ MP$$

$$\frac{\neg mKnown(sk) => \neg cKnown(sk) \qquad \neg mKnown(sk)\ \{Key\ inside\ enclave\}}{\neg cKnown(sk)}\ MP$$

$$Finally,$$
$$Let,\ pTxt = [nonce].\ Then,$$

$$\frac{\dfrac{Lemma\ 6}{\{sk/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\ \forall E \qquad \neg cKnown(sk)\ \{Prev\ Step\} \qquad cKnown(Enc(sk, pTxt))}{\neg mKnown(sk) => \neg cKnown(sk)}\ MP$$

$$\frac{\neg mKnown(sk) => \neg cKnown(sk) \qquad \neg mKnown(sk)\ \{Key\ inside\ enclave\}}{\neg cKnown(sk)}\ MP$$

$$At\ the\ previous\ step,$$

$$\frac{\dfrac{Lemma\ 11}{\{nonce/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 8}{\{sk/key\}\{pTxt/msgSeq\}(Lemma\ 8)}\ \forall E \qquad \neg cKnown(sk)\ \{Proved\} \qquad cKnown(Enc(sk, pTxt))}{\neg mKnown(pTxt) => \neg cKnown(pTxt)}\ MP$$

$$\dfrac{\neg mKnown(pTxt) => \neg cKnown(pTxt) \qquad \neg mKnown(pTxt)}{\neg cKnown(pTxt)}\ MP$$

$$Thus,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{nonce/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{nonce/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(nonce)}\ MP$$

- $EndExecutionInsideEnclave()$
- $Send(Database,\ m_7)$

Postconditions:

$$\neg cKnown(Seed_{Server})$$
$$\neg cKnown(cKey)$$
$$\neg cKnown(SVC_{Passwd})$$
$$\neg cKnown(SK_{Svc})$$
$$\neg cKnown(nonce)$$

4.3.9 EPOCH 7

Preconditions:

$$\neg cKnown(Svc_{Passwd})\ \{Previous\ Epoch\}$$
$$\neg cKnown(SK_{Svc})\ \{Previous\ Epoch\}$$
$$\neg cKnown(cKey)\ \{Previous\ Epoch\}$$
$$\neg cKnown(nonce)\ \{Previous\ Epoch\}$$
$$\neg cKnown(query)\ \{Previous\ Epoch\}$$

- $Receive(Server,\ m_7)$

$$cKnown(m_7)\ \{Prev\ Epoch\}$$

- $CopyInsideEnclave(m_7)$

- $BeginExecutionInsideEnclave()$

$$m_7 = [SvcTkt, Auth, Nonce]$$

- $DecSvcTkt = Dec(Svc_{Passwd}, SvcTkt)$

$$DecSvcTkt = [uname, IPServer, timestamp, lifespan, SK_{Svc}, cKey, query]$$

$$\cfrac{\cfrac{Lemma\ 11}{\{SK_{Svc}/msg\}\{DecSvcTkt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\}}{\neg cKnown(DecSvcTkt)}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{SK_{Svc}/msg\}\{DecSvcTkt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ step\} \qquad \neg cKnown(DecSvcTkt)}{\neg cKnown(SK_{Svc})}\ MP$$

$$Also,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{cKey/msg\}\{DecSvcTkt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(cKey)\ \{Prev\ step\}}{\neg cKnown(DecSvcTkt)}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{cKey/msg\}\{DecSvcTkt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(cKey)\ \{Prev\ step\} \qquad \neg cKnown(DecSvcTkt)}{\neg cKnown(cKey)}\ MP$$

$$and,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{query/msg\}\{DecSvcTkt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(DecSvcTkt)}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{query/msg\}\{DecSvcTkt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\} \qquad \neg cKnown(DecSvcTkt)}{\neg cKnown(query)}\ MP$$

$$Thus,$$

$$\cfrac{\neg cKnown(query)}{\neg cKnown(CK)}\ Proved\ before$$

$$\neg cKnown(Svc_{Passwd})\ \{Previous\ Epoch\ \&\ Inside\ Enclave\}$$

- $DecAuth = Dec(SK_{Svc}, Auth)$

$$DecAuth = [uname, IPServer]$$

$$\cfrac{cKnown(uname) \qquad cKnown(IPServer)}{cKnown(DecAuth)}\ All\ Components\ Known$$

$$Also,$$

$$\neg cKnown(SK_{Svc})\ \{Inside\ Enclave\ \&\ Previous\ Epochs\}$$

- $Validation\ for\ uname\ and\ IPServer$
- $Validation\ for\ timestamp\ and\ lifespan$
- $DecNonce = Dec(SK_{Svc}, Nonce)$

$$DecNonce = [nonce]$$

$$\neg cKnown(nonce)\ \{Previous\ Epoch\}$$

$$\neg cKnown(SK_{Svc})\ \{Previous\ Epoch\ \&\ Inside\ Enclave\}$$

- $m_8 = Enc(SK_{Svc}, [nonce + 1])$

$$Let,\ pTxt = [nonce + 1].\ Then,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{nonce/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Also,$$

$$\cfrac{\cfrac{Lemma\ 7}{\{SK_{Svc}/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(SK_{Svc}, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(SK_{Svc}, pTxt)) => \neg cKnown(Enc(SK_{Svc}, pTxt))}\ MP$$

$$\cfrac{\neg mKnown(Enc(SK_{Svc}, pTxt)) => \neg cKnown(Enc(SK_{Svc}, pTxt)) \qquad \neg mKnown(Enc(SK_{Svc}, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(SK_{Svc}, pTxt))}\ MP$$

$$\cfrac{\cfrac{Lemma\ 9}{\{SK_{Svc}/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Precondition\} \qquad \neg cKnown(Enc(SK_{Svc}, pTxt))}{\neg mKnown(SK_{Svc}) => \neg cKnown(SK_{Svc})}\ MP$$

$$\cfrac{\neg mKnown(SK_{Svc}) => \neg cKnown(SK_{Svc}) \qquad \neg mKnown(SK_{Svc})\ \{Inside\ enclave\}}{\neg cKnown(SK_{Svc})}\ MP$$

- $CopyOutsideEnclave(m_8)$

$$Let,\ pTxt = [nonce + 1].\ Then,$$

$$\cfrac{\cfrac{Lemma\ 6}{\{SK_{Svc}/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ Step\} \qquad cKnown(Enc(SK_{Svc}, pTxt))}{\neg mKnown(SK_{Svc}) => \neg cKnown(SK_{Svc})}\ MP$$

$$\cfrac{\neg mKnown(SK_{Svc}) => \neg cKnown(SK_{Svc}) \qquad \neg mKnown(SK_{Svc})\ \{Key\ inside\ enclave\}}{\neg cKnown(SK_{Svc})}\ MP$$

$$At\ the\ previous\ step,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{nonce/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 8}{\{SK_{Svc}/key\}\{pTxt/msgSeq\}(Lemma\ 8)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Proved\} \qquad cKnown(Enc(SK_{Svc}, pTxt))}{\neg mKnown(pTxt) => \neg cKnown(pTxt)}\ MP$$

$$\dfrac{\neg mKnown(pTxt) => \neg cKnown(pTxt) \qquad \neg mKnown(pTxt)}{\neg cKnown(pTxt)}\ MP$$

$$Thus,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{nonce/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{nonce/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(nonce)}\ MP$$

- $EndExecutionInsideEnclave()$
- $Send(Server,\ m_8)$

Postconditions:

$$\neg cKnown(nonce)$$
$$\neg cKnown(query)$$
$$\neg cKnown(CK)$$
$$\neg cKnown(SK_{Svc})$$
$$\neg cKnown(Svc_{Passwd})$$

4.3.10 EPOCH 8

Preconditions:

$$\neg cKnown(SK_{Svc})\ \{Previous\ Epoch\}$$
$$\neg cKnown(nonce)\ \{Previous\ Epoch\}$$
$$\neg cKnown(query)\ \{Previous\ Epoch\}$$

- $Receive(Database,\ m_8)$

$$cKnown(m_8)\ \{Prev\ Epoch\}$$

- $CopyInsideEnclave(m_8)$
- $BeginExecutionInsideEnclave()$
- $m_8' = Dec(SK_{Svc}, m_8)$

$$m'_8 = [nonce + 1]$$

$$\cfrac{\cfrac{Lemma\ 11}{\{nonce/msg\}\{m'_8/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\}}{\neg cKnown(m'_8)}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{nonce/msg\}\{m'_8/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\} \qquad \neg cKnown(m'_8)}{\neg cKnown(nonce)}\ MP$$

$$\neg cKnown(SK_{Svc})\ \{Previous\ Epoch\ \&\ Inside\ Enclave\}$$

- $Check\ for\ m'_8 = [nonce + 1]$
- $m_9 = Enc(SK_{Svc}, [query])$

$$Let,\ pTxt = [query].\ Then,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Also,$$

$$\cfrac{\cfrac{Lemma\ 7}{\{SK_{Svc}/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(SK_{Svc}, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(SK_{Svc}, pTxt)) => \neg cKnown(Enc(SK_{Svc}, pTxt))}\ MP$$

$$\cfrac{\neg mKnown(Enc(SK_{Svc}, pTxt)) => \neg cKnown(Enc(SK_{Svc}, pTxt)) \qquad \neg mKnown(Enc(SK_{Svc}, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(SK_{Svc}, pTxt))}\ MP$$

$$\cfrac{\cfrac{Lemma\ 9}{\{SK_{Svc}/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Precondition\} \qquad \neg cKnown(Enc(SK_{Svc}, pTxt))}{\neg mKnown(SK_{Svc}) => \neg cKnown(SK_{Svc})}\ MP$$

$$\cfrac{\neg mKnown(SK_{Svc}) => \neg cKnown(SK_{Svc}) \qquad \neg mKnown(SK_{Svc})\ \{Inside\ enclave\}}{\neg cKnown(SK_{Svc})}\ MP$$

$$and,$$

$$\cfrac{\neg cKnown(query)}{\neg cKnown(CK)}\ \{Proved\ above\}$$

- $CopyOutsideEnclave(m_9)$

$$Let,\ pTxt = [query].\ Then,$$

$$\cfrac{\cfrac{Lemma\ 6}{\{SK_{Svc}/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Prev\ Step\} \qquad cKnown(Enc(SK_{Svc}, pTxt))}{\neg mKnown(SK_{Svc}) => \neg cKnown(SK_{Svc})}\ MP$$

$$\cfrac{\neg mKnown(SK_{Svc}) => \neg cKnown(SK_{Svc}) \qquad \neg mKnown(SK_{Svc})\ \{Key\ inside\ enclave\}}{\neg cKnown(SK_{Svc})}\ MP$$

$$At\ the\ previous\ step,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{nonce/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 8}{\{SK_{Svc}/key\}\{pTxt/msgSeq\}(Lemma\ 8)}\ \forall E \qquad \neg cKnown(SK_{Svc})\ \{Proved\} \qquad cKnown(Enc(SK_{Svc}, pTxt))}{\neg mKnown(pTxt) => \neg cKnown(pTxt)}\ MP$$

$$\dfrac{\neg mKnown(pTxt) => \neg cKnown(pTxt) \qquad \neg mKnown(pTxt)}{\neg cKnown(pTxt)}\ MP$$

$$Thus,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(query)}\ MP$$

$$and,$$

$$\dfrac{\neg cKnown(query)}{\neg cKnown(CK)}\ \{Proved\ above\}$$

- $EndExecutionInsideEnclave()$
- $Send(Database,\ m_9)$

Postconditions:

$$\neg cKnown(query)$$

$$\neg cKnown(SK_{Svc})$$

$$\neg cKnown(CK)$$

4.3.11 EPOCH 9

Preconditions:

$$\neg cKnown(SK_{Svc})\ \{Previous\ Epoch\}$$
$$\neg cKnown(cKey)\ \{Previous\ Epoch\}$$
$$\neg cKnown(query)\ \{Previous\ Epoch\}$$

- $Receive(Server,\ m_9)$

$$cKnown(m_9)\ \{Prev\ Epoch\}$$

- $CopyInsideEnclave(m_9)$
- $BeginExecutionInsideEnclave()$
- $m'_9 = Dec(SK_{Svc}, m_9)$

$$m'_9 = query$$

$$\dfrac{\dfrac{Lemma\ 11}{\{query/msg\}\{m'_9/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(m'_9)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{query/msg\}\{m'_9/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\} \qquad \neg cKnown(m'_9)}{\neg cKnown(query)}\ MP$$

$$\neg cKnown(SK_{Svc})\ \{Previous\ Epoch\ \&\ Inside\ Enclave\}$$

$$Also,$$

$$\neg cKnown(CK)\ \{Precondition\}$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 7}{\{CK/key\}\{Query/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(CK, Query))\ \{Precondition\}}{\neg mKnown(Enc(CK, Query)) => \neg cKnown(Enc(CK, Query))}\ MP$$

$$\dfrac{\neg mKnown(Enc(CK, Query)) => \neg cKnown(Enc(CK, Query)) \qquad \neg mKnown(Enc(CK, Query))\ \{Inside\ enclave\}}{\neg cKnown(Enc(CK, Query))}\ MP$$

$$\dfrac{\dfrac{Lemma\ 9}{\{CK/key\}\{Query/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(CK)\ \{Precondition\} \qquad \neg cKnown(Enc(CK, Query))}{\neg mKnown(CK) => \neg cKnown(CK)}\ MP$$

$$\dfrac{\neg mKnown(CK) => \neg cKnown(CK) \qquad \neg mKnown(CK)\ \{Inside\ enclave\}}{\neg cKnown(CK)}\ MP$$

- $q = Dec(cKey, query)$

$$cKey = CK$$

$$q = Query$$

$$\cfrac{\cfrac{Lemma\ 11}{\{Query/msg\}\{q/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(Query)\ \{Prev\ step\}}{\neg cKnown(q)}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{Query/msg\}\{q/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(Query)\ \{Prev\ step\} \qquad \neg cKnown(q)}{\neg cKnown(Query)}\ MP$$

$$\neg cKnown(CK)\ \{Previous\ Epoch\ \&\ Inside\ Enclave\}$$

- $result = execute(q)$

$$Assumption\ that\ query\ execution\ is\ privacy\ preserving$$

- $m_{10} = Enc(cKey, [result, query])$

$$Let,\ pTxt = [result, query].\ Then,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Also,$$

$$\cfrac{\cfrac{Lemma\ 7}{\{cKey/key\}\{pTxt/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(cKey, pTxt))\ \{vacuity\}}{\neg mKnown(Enc(cKey, pTxt)) => \neg cKnown(Enc(cKey, pTxt))}\ MP$$

$$\cfrac{\neg mKnown(Enc(cKey, pTxt)) => \neg cKnown(Enc(cKey, pTxt)) \qquad \neg mKnown(Enc(cKey, pTxt))\ \{Inside\ enclave\}}{\neg cKnown(Enc(cKey, pTxt))}\ MP$$

$$\cfrac{\cfrac{Lemma\ 9}{\{cKey/key\}\{pTxt/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(cKey)\ \{Precondition\} \qquad \neg cKnown(Enc(cKey, pTxt))}{\neg mKnown(cKey) => \neg cKnown(cKey)}\ MP$$

$$\cfrac{\neg mKnown(cKey) => \neg cKnown(cKey) \qquad \neg mKnown(cKey)\ \{Inside\ enclave\}}{\neg cKnown(cKey)}\ MP$$

$$and,$$

$$\cfrac{\neg cKnown(query)}{\neg cKnown(CK)}\ \{Proved\ above\}$$

- $CopyOutsideEnclave(m_{10})$

$$Let,\ pTxt = [query].\ Then,$$

$$\dfrac{\dfrac{Lemma\ 6}{\{cKey/key\}\{pTxt/msgSeq\}(Lemma\ 6)}\ \forall E \qquad \neg cKnown(cKey)\ \{Prev\ Step\} \qquad cKnown(Enc(cKey, pTxt))}{\neg mKnown(cKey) => \neg cKnown(cKey)}\ MP$$

$$\dfrac{\neg mKnown(cKey) => \neg cKnown(cKey) \qquad \neg mKnown(cKey)\ \{Key\ inside\ enclave\}}{\neg cKnown(cKey)}\ MP$$

$$At\ the\ previous\ step,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{nonce/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(nonce)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$Then,$$

$$\dfrac{\dfrac{Lemma\ 8}{\{cKey/key\}\{pTxt/msgSeq\}(Lemma\ 8)}\ \forall E \qquad \neg cKnown(cKey)\ \{Proved\} \qquad cKnown(Enc(cKey, pTxt))}{\neg mKnown(pTxt) => \neg cKnown(pTxt)}\ MP$$

$$\dfrac{\neg mKnown(pTxt) => \neg cKnown(pTxt) \qquad \neg mKnown(pTxt)}{\neg cKnown(pTxt)}\ MP$$

$$Thus,$$

$$\dfrac{\dfrac{Lemma\ 11}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(pTxt)}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{query/msg\}\{pTxt/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\} \qquad \neg cKnown(pTxt)}{\neg cKnown(query)}\ MP$$

$$and,$$

$$\dfrac{\neg cKnown(query)}{\neg cKnown(CK)}\ \{Proved\ above\}$$

- $EndExecutionInsideEnclave()$
- $Send(Server,\ m_{10})$

Postconditions:

$$\neg cKnown(query)$$

$$\neg cKnown(result)$$

$$\neg cKnown(CK)$$

4.3.12 EPOCH 10

Preconditions:

$$\neg cKnown(cKey)\ \{Previous\ Epoch\}$$

$$\neg cKnown(result)\ \{Previous\ Epoch\}$$

$$\neg cKnown(query)\ \{Previous\ Epoch\}$$

- $Receive(Database,\ m_{10})$

$$cKnown(m_{10})\ \{Prev\ Epoch\}$$

- $Send(Client,\ m_{10})$

Postconditions:

$$\neg cKnown(query)$$

$$\neg cKnown(Query)$$

$$\neg cKnown(result)$$

$$\neg cKnown(CK)$$

4.3.13 EPOCH 11

Preconditions:

$$\neg cKnown(cKey)\ \{Previous\ Epoch\}$$

$$\neg cKnown(result)\ \{Previous\ Epoch\}$$

$$\neg cKnown(query)\ \{Previous\ Epoch\}$$

$$\neg cKnown(Query)\ \{Previous\ Epoch\}$$

- $Receive(Server,\ m_{10})$

$$cKnown(m_{10})\ \{Prev\ Epoch\}$$

- $m'_{10} = Dec(CK, m_{10})$

$$m'_{10} = [result, query]$$

$$\dfrac{\dfrac{Lemma\ 11}{\{query/msg\}\{m'_{10}/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\}}{\neg cKnown(m'_{10})}\ MT$$

$$\dfrac{\dfrac{Lemma\ 10}{\{query/msg\}\{m'_{10}/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(query)\ \{Prev\ step\} \qquad \neg cKnown(m'_{10})}{\neg cKnown(query)}\ MP$$

$$and,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{result/msg\}\{m'_{10}/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(result)\ \{Prev\ step\}}{\neg cKnown(m'_{10})}\ MT$$

$$\cfrac{\cfrac{Lemma\ 10}{\{result/msg\}\{m'_{10}/msgSeq\}(Lemma\ 10)}\ \forall E \qquad \neg cKnown(result)\ \{Prev\ step\} \qquad \neg cKnown(m'_{10})}{\neg cKnown(result)}\ MP$$

$$\neg cKnown(CK)\ \{Precondition\}$$

$$Then,$$

$$\cfrac{\cfrac{Lemma\ 7}{\{CK/key\}\{Query/msgSeq\}(Lemma\ 7)}\ \forall E \qquad \neg cKnown(Enc(CK, Query))\ \{Precondition\}}{\neg mKnown(Enc(CK, Query)) => \neg cKnown(Enc(CK, Query))}\ MP$$

$$\cfrac{\neg mKnown(Enc(CK, Query)) => \neg cKnown(Enc(CK, Query)) \qquad \neg mKnown(Enc(CK, Query))\ \{Inside\ enclave\}}{\neg cKnown(Enc(CK, Query))}\ MP$$

$$\cfrac{\cfrac{Lemma\ 9}{\{CK/key\}\{Query/msgSeq\}(Lemma\ 9)}\ \forall E \qquad \neg cKnown(CK)\ \{Precondition\} \qquad \neg cKnown(Enc(CK, Query))}{\neg mKnown(CK) => \neg cKnown(CK)}\ MP$$

$$\cfrac{\neg mKnown(CK) => \neg cKnown(CK) \qquad \neg mKnown(CK)\ \{Inside\ enclave\}}{\neg cKnown(CK)}\ MP$$

$$Finally,$$

$$\cfrac{\cfrac{Lemma\ 11}{\{Query/msg\}\{[Query]/msgSeq\}(Lemma\ 11)}\ \forall E \qquad \neg cKnown(Query)\ \{Prev\ step\}}{\neg cKnown([Query])}\ MT$$

$$Then,$$

$$\cfrac{\cfrac{Lemma\ 8}{\{CK/key\}\{[Query]/msgSeq\}(Lemma\ 8)}\ \forall E \qquad \neg cKnown(CK)\ \{Proved\} \qquad cKnown(Enc(CK, [Query]))}{\neg mKnown([Query]) => \neg cKnown([Query])}\ MP$$

$$\cfrac{\neg mKnown([Query]) => \neg cKnown([Query]) \qquad \neg mKnown([Query])}{\neg cKnown([Query])}\ MP$$

- *Check that the query received was the one sent*
- *Obtain Result*
- $EndExecutionInsideEnclave()$

Postconditions:

$$\neg cKnown(Query)$$

$$\neg cKnown(result)$$

$$\neg cKnown(CK)$$