BAN Logic Notation and Rules

We used the following notations for the formal analysis based on BAN logic:

- the statement A believes X, will be denoted as $A \mid\equiv X$,
- the statement A received X, will be denoted as $A \lhd X$,
- the statement X is fresh, will be denoted as $\#(X)$,
- the statement A said X once, will be denoted as $A \mid\sim X$,
- the statement A has jurisdiction over X will be denoted as $A \mid\Rightarrow X$,
- the statement A and B communicate with each other using shared key K will be denoted as $A \overset{K}{\leftrightarrow} B$.

Also, X and Y will be denoted in the statements, and A and B will be denoted in the communication participants. Additionally, we used the following BAN logic rules:

1. R1 (message meaning): $\frac{A|\equiv A \overset{K}{\leftrightarrow} B, A \lhd \{X\}_K}{A|\equiv B|\sim X}$, which means that A believes that key K is shared with user B and X is encrypted by K, so user A believes that user B once said X,
2. R2 (freshness): $\frac{A|\equiv \#(X)}{A|\equiv \#(X,Y)}$, which confirms that the whole statement is fresh if one part of it is fresh,
3. R3 (identifier verification): $\frac{A|\equiv \#(X), A|\equiv B|\sim X}{A|\equiv B|\equiv X}$, which means that A believes B believes X, so X is fresh,
4. R4 (jurisdiction): $\frac{A|\equiv B \Rightarrow X, A|\equiv B|\equiv X}{A|\equiv X}$, which means user A believes that user B has authority over X, also user A trusts that user B beliefs on X,
5. R5 (belief): $\frac{A|\equiv B|\equiv (X,Y)}{A|\equiv B|\equiv (X)}$, which means that if the user A sees a statement, he also see all of the components,
6. R6 (shared key): $\frac{A|\equiv B|\equiv X}{A|\equiv A \overset{K}{\leftrightarrow} B}$, which means that user A trusts that user B beliefs on X if user A believe that A and B communicate with each other using shared key K.

Next, based on BAN logic, we assumed that our protocol should satisfy the following goals:

- G1: $D \mid\equiv (D \overset{K}{\leftrightarrow} D_{MI})$, which means that each device must believe that K is shared between them and meeting initiator.
- G2: $S \mid\equiv (D_{MI} \overset{K}{\leftrightarrow} D)$, which means that meeting initiator must believe that K is shared between them and device D.
- G3: $D \mid\equiv D_{MI} \mid\equiv (D \overset{K}{\leftrightarrow} S)$, which means that each device must believe that the meeting initiator believes that K is shared between them.
- G4: $S \mid\equiv D \mid\equiv (D \overset{K}{\leftrightarrow} D_{MI})$, which means that the meeting initiator must believe that device D believe that K is shared between them.

Initial Phase Analysis Ysing BAN Logic

For the initial phase of our protocol, we made the following assumptions:

- A1: $D \mid\equiv \#hash(i(D))$, which means that device D believe that $\#hash(i(D))$ is fresh, because it is generated by them.
- A2: $D \mid\equiv \#(T_D)$, which means that device D believe that T_D is fresh, because it is generated by them.
- A3: $D \mid\equiv D \xleftrightarrow{K_{DS}} S$, which means that device D can verify the legitimacy of the messages sent by server S since they share the key K_{SD}.
- A4: $S \mid\equiv D \xleftrightarrow{K_{DS}} S$, which means that server S can verify the legitimacy of the messages sent by device D since they share the key K_{SD}.
- A5: $S \mid\equiv \#(T_S)$, which means that server S believe that T_S if fresh, because it is generated by them.
- A6: $S \mid\equiv D \Rightarrow S \xleftrightarrow{K_{DS}} S$, which means that after checking in α_3 step whether T_D and T_D are equal to their substitutes in server's knowledge, server S believes that device D has jurisdiction on the information that device and server are using the same key K_{DS}.
- A7: $D \mid\equiv \#(T_S)$, which means that device D believe that T_S is fresh because T_S is the current server's timestamp, and the device can verify its status.
- A8: $D \mid\equiv K_{DS}$, which means that device D believe that K_{DS} is fresh because it is sent with the current server's timestamp.
- A9: $S \mid\equiv \#hash(i(D))$, which means that server S believe that $\#hash(i(D))$ is fresh because T_D is the current device's timestamp, and the device can verify its status.

After analysing our protocol's initial phase using BAN logic, our observations are as follows.

- O1 (based on steps α_1, α_3): $S \lhd \{\#hash(i(D)), T_D\}$,
- O2 (based on O1, R1): $S \mid\equiv D \mid\sim \{\#hash(i(D)), T_D\}$,
- O3 (based on O2, R2, A9): $S \mid\equiv D \mid\equiv \{T_D\}$,
- O4 (based on O3, R5): $S \mid\equiv D \mid\equiv T_D$,
- O5 (based on R6): $S \mid\equiv D \mid\equiv D \xleftrightarrow{K_{DS}} S$ (G4 achieved),
- O6 (based on O5, R4, A4): $S \mid\equiv D \xleftrightarrow{K_{DS}} S$ (G3 achieved),
- O7 (based on steps α_2): $D \lhd \{T_S, K_{DS}\}$,
- O8 (based on O7, A3, R1): $D \mid\equiv S \mid\sim \{T_S, K_{DS}\}$,

- O9 (based on O8, R2, A7): $D \mid\equiv S \mid\equiv \{T_S\}$,
- O10 (based on R6): $D \mid\equiv S \mid\equiv D \xleftrightarrow{K_{DS}} S$ (G2 achieved),
- O11 (based on O10, R4, A3): $D \mid\equiv D \xleftrightarrow{K_{DS}} S$ (G1 achieved)

Session Key Establishment Phase Analysis Using BAN Logic

For the session key establishment phase of our protocol, we made the following assumptions:

- A1: $S \mid\equiv K_{D_{MI}D}$, which means that server S believe that $K_{D_{MI}D}$ is fresh, because it is generated by them.
- A2: $D_{MI} \mid\equiv D_{MI}D_{MI} \xleftrightarrow{D_{MI}S} S$, which means that the meeting initiator D_{MI} can verify the legitimacy of the messages sent by server S since they share the key $K_{D_{MI}S}$.
- A3: $S \mid\equiv D_{MI} \xleftrightarrow{K_{D_{MI}S}} S$, which means that server S can verify the legitimacy of the messages sent by the meeting initiator D_{MI} since they share the key $K_{D_{MI}S}$.
- A4: $S \mid\equiv \#(T_S)$, which means that server S believe that T_S if fresh, because it is generated by them.
- A5: $S \mid\equiv D \Rightarrow S \xleftrightarrow{K_{DS}} S$, which means that after checking in α_4 step whether T_S is equal to its substitute in the server's knowledge, the server s believes that device D has jurisdiction on the information that device and server are using the same key K_{DS}.
- A6: $D \mid\equiv \#(T_S)$, which means that device D believe that T_S is fresh because T_S is the current server's timestamp, and the device can verify its status.
- A7: $S \mid\equiv T_S$, which means that server S believe that T_S is fresh, because it is generated by them.
- A8: $D_{MI} \mid\equiv T_{D_{MI}}$, which means that the meeting initiator D_{MI} believes that $T_S D_{MI}$ is fresh, because it is generated by them.
- A9: $S \mid\equiv K_{D_{MI}S}$, which means that device D believes that $K_{D_{MI}S}$ is fresh because it is sent with the current device's timestamp.
- A10: $S \mid\equiv \#(T_{D_{MI}})$, which means that server S believe that $T_{D_{MI}}$ is fresh because $T_{D_{MI}}$ is the current device's timestamp, and the device can verify its status.

After analysing our protocol's session key establishment phase using BAN logic, our observations are as follows.

- O1 (based on steps α_1, α_4): $S \lhd \{T_{D_{MI}},$
  $\#hash(i(D_{MI})), \#hash(i(D)), T_S\}$,

- O2 (based on O1, R1): $S \mid\equiv D_{MI} \mid\sim \{T_{D_{MI}}$,
$\#hash(i(D_{MI})), \#hash(i(D))\}$,
- O3 (based on O2, R2, A8): $S \mid\equiv D_{MI} \mid\equiv \{T_{D_{MI}}\}$,
- O4 (based on O3, R5): $S \mid\equiv D \mid\equiv T_{D_{MI}}$,
- O5 (based on R6): $S \mid\equiv D \mid\equiv D \xleftrightarrow{K_{DS}} S$ (G4 achieved),
- O6 (based on R6): $S \mid\equiv D_{MI} \mid\equiv D_{MI} \xleftrightarrow{K_{D_{MI}S}} S$ (G4 achieved),
- O7 (based on O5, R4, A3): $S \mid\equiv D \xleftrightarrow{K_{DS}} S$ (G3 achieved),
- O8 (based on O5, R4, A3): $S \mid\equiv D_{MI} \xleftrightarrow{K_{D_{MI}S}} S$ (G3 achieved),
- O9 (based on steps α_3): $D \triangleleft \{T_S, \#hash(i(D_{MI}))\}$,
- 010 (based on O7, A2, R1): $D \mid\equiv S \mid\sim \{T_S$,
$\#hash(i(D_{MI}))\}$,
- 011 (based on O8, R2, A6): $D \mid\equiv S \mid\equiv \{T_S\}$,
- O12 (based on R6): $D \mid\equiv S \mid\equiv D \xleftrightarrow{K_{DS}} S$ (G2 achieved),
- O13 (based on R6): $D_{MI} \mid\equiv S \mid\equiv D_{MI} \xleftrightarrow{K_{D_{MI}S}} S$ (G2 achieved),
- O14 (based on O10, R4, A2): $D \mid\equiv D \xleftrightarrow{K_{DS}} S$ (G1 achieved),
- O15 (based on O10, R4, A2): $D_{MI} \mid\equiv D_{MI} \xleftrightarrow{K_{D_{MI}S}} S$ (G1 achieved),

Communication Phase Analysis Using BAN Logic

For the communication phase of our protocol, we made the following assumptions:

- A1: $D \mid\equiv \#(P)$, which means that device D believe that P is fresh, because it is generated by them.
- A2: $D \mid\equiv \#(T_D)$, which means that device D believe that T_D is fresh, because it is generated by them.
- A3: $D \mid\equiv D \xleftrightarrow{K_{D_{MI}D}} D_{MI}$, which means that the device D can verify the legitimacy of the messages sent by the meeting initiator D_{MI} since they share the key $K_{D_{MI}D}$.
- A4: $D_{MI} \mid\equiv D \xleftrightarrow{K_{D_{MI}D}} S$, which means that the meeting initiator D_{MI} can verify the legitimacy of the messages sent by device D since they share the key $K_{D_{MI}D}$.
- A5: $D_{MI} \mid\equiv \#(T_{D_{MI}})$, which means that the meeting initiator D_{MI} believes that $T_{D_{MI}}$ if fresh, because it is generated by them.

- A6: $D \mid\equiv \#(T_{D_{MI}})$, which means that device D believe that $T_{D_{MI}}$ is fresh because $T_{D_{MI}}$ is the current meeting initiator's timestamp, and the device can verify its status.
- A7: $D_{MI} \mid\equiv D \Rightarrow D_{MI} \xleftrightarrow{K_{D_{MI}D}} D_{MI}$, which means that after checking in α_2 step whether $\#hash(i(D))$ is equal to their substitutes in the meeting initiator server's knowledge, the meeting initiator believes that device D has jurisdiction on the information that device and server are using the same key $K_{D_{MI}D}$.
- A8: $D \mid\equiv GC_{MI}$ means that device D believe that GC_{MI} is fresh because it is sent with the current meeting initiator's timestamp.
- A9: $D \mid\equiv P_{MI}$ means that device D believe that P_{MI} is fresh because it is sent with the current meeting initiator's timestamp.

After analysing our protocol's communication phase using BAN logic, our observations are as follows.

- O1 (based on steps α_2, α_4): $D_{MI} \triangleleft \{\#hash(i(D)), GC, P, T_D\}$,
- O2 (based on O1, R1): $D_{MI} \mid\equiv D \mid\sim \{\#hash(i(D)), GC, P, T_D\}$,
- O3 (based on O2, R2, A8, A9): $D_{MI} \mid\equiv D \mid\equiv \{\#hash(i(D_{MI})), GC_{D_{MI}}, P_{D_{MI}}, T_{D_{MI}}, GC^2_{D_{MI}}, P^2_{D_{MI}}\}$,
- O4 (based on O3, R5): $D_{MI} \mid\equiv D \mid\equiv T_D$,
- O5 (based on R6): $D_{MI} \mid\equiv D \mid\equiv D \xleftrightarrow{K_{D_{MI}D}} S$ (G4 achieved),
- O6 (based on O5, R4, A4): $D_{MI} \mid\equiv D \xleftrightarrow{K_{D_{MI}D}} S$ (G3 achieved),
- O7 (based on steps α_1, α_3): $D \triangleleft \{\#hash(i(D_{MI})), T_{D_{MI}}, GC_{D_{MI}}, P_{D_{MI}}, GC^2_{D_{MI}}\}$,
- O8 (based on O7, A3, R1): $D \mid\equiv D_{MI} \mid\sim \{T_{D_{MI}}, K_{SD}\}$,
- O9 (based on O8, R2, A7): $D \mid\equiv D_{MI} \mid\equiv \{T_{D_{MI}}, K_{SD}\}$,
- O10 (based on R6): $D \mid\equiv D_{MI} \mid\equiv D \xleftrightarrow{K_{D_{MI}D}} D_{MI}$ (G2 achieved),
- O11 (based on O10, R4, A3): $D \mid\equiv D \xleftrightarrow{K_{D_{MI}D}} D_{MI}$ (G1 achieved)