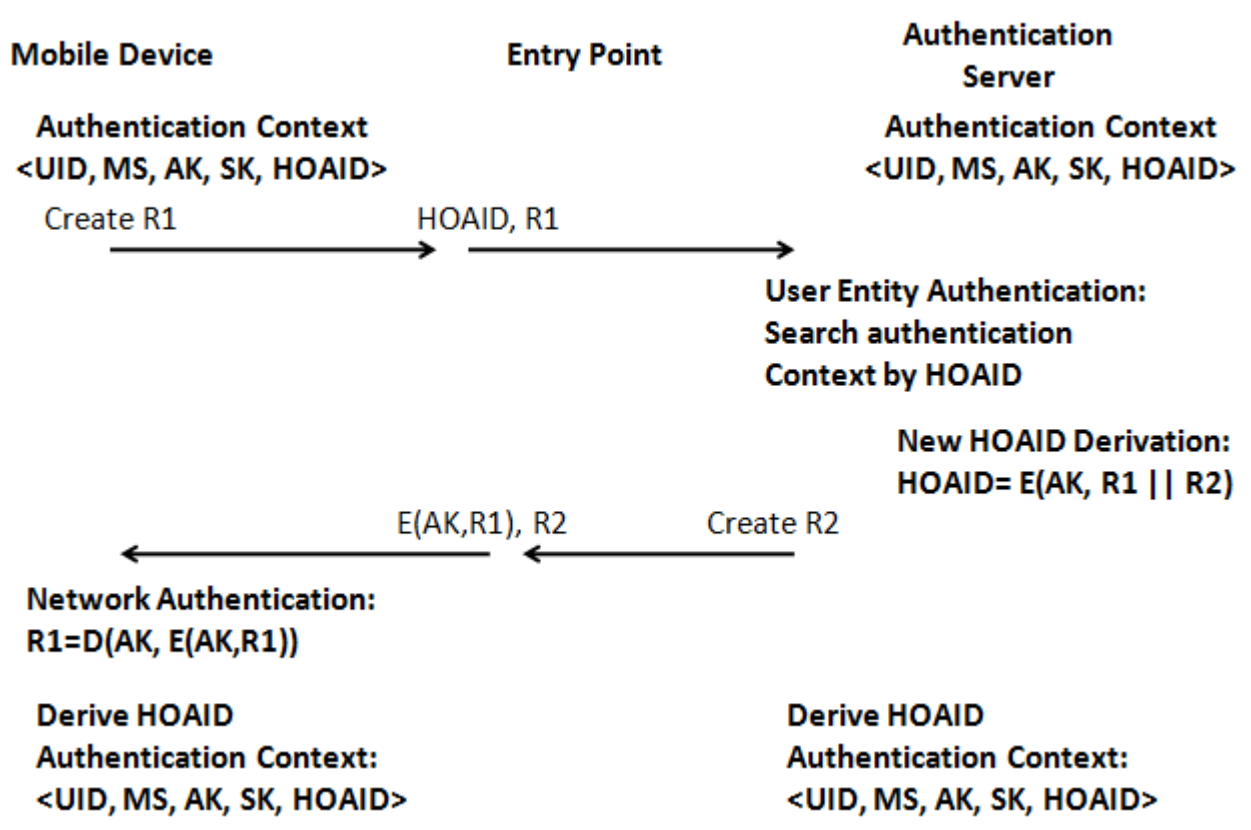
Mobile Device
Entry Point
Authentication Server
Authentication Context
<UID, MS, AK, SK, HOAID>
Authentication Context
<UID, MS, AK, SK, HOAID>
Create R1
HOAID, R1
User Entity Authentication:
Search authentication
Context by HOAID
New HOAID Derivation:
HOAID= E(AK, R1 || R2)
E(AK,R1), R2
Create R2
Network Authentication:
R1=D(AK, E(AK,R1))
Derive HOAID
Authentication Context:
<UID, MS, AK, SK, HOAID>
Derive HOAID
Authentication Context:
<UID, MS, AK, SK, HOAID>