```
free c, c_fs, c_iot: channel.
free c_secure: channel [private].

free SN1, SN2: bitstring [private].
free IDm: bitstring.

fun h(bitstring): bitstring.
fun concat(bitstring, bitstring): bitstring.
fun xor(bitstring, bitstring): bitstring.

equation forall x: bitstring, y: bitstring; xor(xor(x, y), y) = x.
equation forall x: bitstring, y: bitstring; xor(x, y) = xor(y, x).

let UserProcess =
  new IDu: bitstring;
 new PWu: bitstring;
 new r1: bitstring;
 new BIOu: bitstring;

 let HPWu = h(concat(concat(IDu, PWu), r1)) in
 let HIBu = h(concat(BIOu, r1)) in

 out(c_secure, (IDu, HPWu, HIBu));

 in(c_secure, (V1: bitstring, V2: bitstring, V3: bitstring, IDDy: bitstring, h_func: bitstring));

 let V4 = xor(r1, h(concat(concat(IDu, PWu), HIBu))) in

 event userStoredCredentials(IDu, IDDy);

  let r1_recovered = xor(V4, h(concat(concat(IDu, PWu), HIBu))) in
 let HPWu_recovered = h(concat(concat(IDu, PWu), r1_recovered)) in
 let HIBu_recovered = h(concat(BIOu, r1_recovered)) in

 let temp1 = xor(V1, h(concat(HPWu_recovered, HIBu_recovered))) in (* h(IDDy||SN1||IDm) *)

 let r2_recovered = xor(V2, temp1) in
 let V3_star = h(concat(concat(HPWu_recovered, r2_recovered), HIBu_recovered)) in

 if V3_star = V3 then (
  new r3: bitstring;
  let W1 = xor(r3, temp1) in
  new T1: bitstring;
  let W2 = h(concat(concat(concat(IDu, SIDiot), V1), T1)) in
  let W3 = h(concat(concat(IDu, SIDiot), h(concat(HPWu_recovered, HIBu_recovered)))) in

  out(c, (W1, W2, W3, IDDy, T1));

  in(c, (X3: bitstring, X4: bitstring, T7: bitstring));

  let X3_star = h(concat(concat(concat(V1_star: bitstring, r4_received: bitstring), r5_received: bitstring), IDDy_star: bitstring)) in

  if X3_star = X3 then (
   let SKu = concat(h(concat(concat(r3, r4_received), r5_received)), h(concat(HPWu_recovered, HIBu_recovered))) in
   let X4_star = h(concat(concat(SKu, V1_star), IDDy_star)) in

   if X4_star = X4 then (
    event userAuthenticationSuccess(IDu);
    out(c, success)
   ) else (
    event userAuthenticationFailure(IDu);
    out(c, failure)
   )
  ) else (
   event userAuthenticationFailure(IDu);
```

```
      out(c, failure)
    )
  ) else (
    event userLoginFailure(IDu);
    out(c, failure)
  ).

let FogServerProcess =
  let Y = h(concat(IDiot, SN1)) in
  let Z = h(concat(concat(Y, SN1), SN2)) in

    event fogInitialized(Y, Z);

  in(c_secure, (IDu_reg: bitstring, HPWu_reg: bitstring, HIBu_reg: bitstring));

  new IDDy_reg: bitstring;
  new r2_reg: bitstring;

  let temp_fs = h(concat(concat(IDDy_reg, SN1), IDm)) in
  let V1_reg = xor(temp_fs, h(concat(HPWu_reg, HIBu_reg))) in
  let V2_reg = xor(r2_reg, temp_fs) in
  let V3_reg = h(concat(concat(HPWu_reg, r2_reg), HIBu_reg)) in

    event fogStoredUser(IDu_reg, IDDy_reg);

  out(c_secure, (V1_reg, V2_reg, V3_reg, IDDy_reg, h));

   in(c, (W1: bitstring, W2: bitstring, W3: bitstring, IDDy_auth: bitstring, T1: bitstring));

    let r2_recovered_fs = xor(V2_stored: bitstring, h(concat(concat(IDDy_auth, SN1), IDm))) in
  let W2_star = h(concat(concat(concat(IDu_retrieved: bitstring, SIDiot), V1_retrieved: bitstring), T1)) in

  if W2_star = W2 then (
    let hHPW_HIB = xor(V1_retrieved, h(concat(concat(IDDy_auth, SN1), IDm))) in
    let W3_star = h(concat(concat(IDu_retrieved, SIDiot), hHPW_HIB)) in

    if W3_star = W3 then (
      new r4: bitstring;
      new T3: bitstring;

      let W4 = xor(r4, concat(hHPW_HIB, T3)) in
      let W5 = h(concat(concat(concat(concat(IDm, IDu_retrieved), r2_recovered_fs), V1_retrieved), T3)) in

      out(c_fs, (W1, W4, W5, T3));

      in(c_fs, (X1: bitstring, X2: bitstring, T5: bitstring));

      let r5 = xor(X1, h(concat(r3_recovered: bitstring, r4))) in
      let SKfn = concat(h(concat(concat(r3_recovered, r4), r5)), hHPW_HIB) in
      let X2_star = h(concat(concat(concat(SKfn, IDu_retrieved), IDm), T5)) in

      if X2_star = X2 then (
        new IDDy_new: bitstring;
        let V1_new = xor(r2_recovered_fs, h(concat(concat(IDDy_new, SN1), IDm))) in
        let X3 = h(concat(concat(concat(V1_new, r4), r5), IDDy_new)) in
        let X4 = h(concat(concat(SKfn, V1_new), IDDy_new)) in
        new T7: bitstring;

        event fogAuthenticationSuccess(IDu_retrieved);
        out(c, (X3, X4, T7))
      ) else (
        event fogAuthenticationFailure(IDu_retrieved);
        out(c, failure)
      )
    ) else (
      event fogVerificationFailure(IDu_retrieved);
      out(c, failure)
    )
  ) else (
    event fogVerificationFailure(IDu_retrieved);
    out(c, failure)
  ).

let IoTDeviceProcess =
  (* Contains pre-loaded {Y, Z} from initialization *)
  let Y_loaded = h(concat(IDiot, SN1)) in
  let Z_loaded = h(concat(concat(Y_loaded, SN1), SN2)) in

  in(c_iot, (W1_iot: bitstring, W4_iot: bitstring, W5_iot: bitstring, T3_iot: bitstring));

  let hHPW_HIB_iot = xor(xor(W1_iot, r3_iot: bitstring), V1_iot: bitstring) in
  let r4_iot = xor(W4_iot, concat(hHPW_HIB_iot, T3_iot)) in
  let W5_star = h(concat(concat(concat(concat(IDm, IDu_iot: bitstring), r2_iot: bitstring), V1_iot), T3_iot)) in

  if W5_star = W5_iot then (
    new r5_iot: bitstring;
    new T5_iot: bitstring;

    let X1_iot = xor(r5_iot, h(concat(r3_iot, r4_iot))) in
    let SKiot = concat(h(concat(concat(r3_iot, r4_iot), r5_iot)), hHPW_HIB_iot) in
    let X2_iot = h(concat(concat(concat(SKiot, IDu_iot), IDm), T5_iot)) in

    event iotAuthenticationSuccess(IDu_iot);
    out(c_iot, (X1_iot, X2_iot, T5_iot))
  ) else (
    event iotAuthenticationFailure(IDu_iot);
    out(c_iot, failure)
  ).
process
  new SIDiot: bitstring;
  new IDiot: bitstring;

 (
    !UserProcess | !FogServerProcess | !IoTDeviceProcess
  )
```