```
theory AKAP begin
builtins: asymmetric-encryption, signing, hashing
/*
Protocol:   A Secure End-to-End Micropayment Protocol for
Wearable Devices
Modeler:   Sriramulu Bojjagani,
Date:         Jan 2022
Status:   Working
*/
// Function signature and definition of the equational theory E
functions: adec/2, aenc/2, fst/1, pair/2, pk/1, sign/2, snd/1,
           true/0, verify/3
equations:
    adec(aenc(x.1, pk(x.2)), x.2) = x.1,
    fst(<x.1, x.2>) = x.1,
    snd(<x.1, x.2>) = x.2,
    verify(sign(x.1, x.2), x.1, pk(x.2)) = true
rule (modulo E) Register_pk:
   [ Fr( ~ltkA ) ]
  -->
   [ !Puk( $A, ~ltkA ), !Pubk( $A, pk(~ltkA) ), Out( pk(~ltkA) ) ]

  /* has exactly the trivial AC variant */
rule (modulo E) Reveal_ltk:
   [ !Puk( A, ltkA ) ] --[ RevLtk( A ) ]-> [ Out( ltkA ) ]

  /* has exactly the trivial AC variant */
rule (modulo E) U_1:
   [ Fr( ~nu ), !Pubk( $FSi, pkFS ), !Sk( $Ui, skU ) ]
  --[ OUT_U_1( sign(<'1', $Ui, ~nu>, skU) ) ]->
   [
   Out( sign(<'1', $Ui, ~nu>, skU) ),
   U_1( <$Ui, ~nu, sign(<'1', $Ui, ~nu>, skU)>, pkFS )
   ]
```

```
/* has exactly the trivial AC variant */
rule (modulo E) FS_1:
   [
   !Pubk( $FSi, ltFS ),
   In( aenc(<nu, Uid, sign(<'1', Uid, nu>, skU)>, pk(ltkFS)) ),
   !FS_data( TS_fs, VN_u,n_u,TS_u), !Sk( $FSi, skFS ),
   !Pubk( IDu, pkS ), Fr( ~nfs )
   ]
  --[
  IN_FS_1_nu( nu, aenc(<nu, Uid, sign(<'1', Uid, nu>, skU)>,
pk(ltkFS))
  ),
  OUT_FS_1( aenc(<nu, ~nfs, $Ui, FSid, TS_fs, VN_u,n_u,TS_u,
                 sign(<'2', nu, ~nfs, $FSi, TS_fs, VN_u,n_u,TS_u>,
skFS)>,
                pkU)
  ),
  Running( Uid, $FSi, <'init', nu, ~nfs, TS_fs, VN_u,n_u,TS_u> )
  ]->
   [
   Out( aenc(<nu, ~nfs, $FSi, TS_fs, VN_u,n_u,TS_u,
              sign(<'2', nu, ~nfs, $FSi, TS_fs, VN_u,n_u,TS_u>,
skFS)>,
             pkU)
   ),
   FS_1( <$FSi, Uid, nu, ~nfs, TS_fs, VN_u,n_u,TS_u,
         sign(<'2', nu, ~nfs, $FSi, TS_fs, VN_u,n_u,TS_u>, skFS)>,
        pkU
   )
   ]
```

```
 /* has exactly the trivial AC variant */

rule (modulo E) Secrecy_claim:
   [ Secret( A, B, fs ) ] --[ Secret( A, B, fs ) ]-> [ ]

  /* has exactly the trivial AC variant */

lemma nonce_secrecy:
  all-traces
  "¬(∃ A B s #i.
      (((Secret( A, B, s ) @ #i) ∧ (∃ #j. K( s ) @ #j)) ∧
       (¬(∃ #r. RevLtk( A ) @ #r))) ∧
      (¬(∃ #r. RevLtk( B ) @ #r)))"
/*
guarded formula characterizing all counter-examples:
"∃ A B s #i.
  (Secret( A, B, s ) @ #i)
 ∧
  (∃ #j. (K( s ) @ #j)) ∧
  (∀ #r. (RevLtk( A ) @ #r) ⇒ ⊥) ∧
  (∀ #r. (RevLtk( B ) @ #r) ⇒ ⊥)"
*/
by sorry

/* All well-formedness checks were successful. */

end
```