authentication based on digital signatures, extended

Protocol Purpose

IKE is designed to perform mutual authentication and key exchange prior to setting up an IPsec connection. IKEv2 exists in several variants, the defining di□erence being the authentication method used.

```
2. State = 2  /\ RCV_
   State':= 4 /\ SA2
              /\ SK'
              /\ SND_
```

```
        a, b       : agent,
        ka, kb, ki : public_key,
        g          : text,
        f          : function,
        zero, one  : text

  intruder_knowledge = {g,f,a,b,ka,kb,i,ki,inv(ki),zero,one
                        }

  composition

        session(a,b,ka,kb,g,f)
     /\ session(a,i,ka,ki,g,f)
     /\ session(i,b,ki,kb,g,f)

end role
```

```
goal

  %secrecy_of SK
  secrecy_of sec_a_SK, sec_b_SK

  %Alice authenticates Bob on sk1
  authentication_on sk1
  %Bob authenticates Alice on sk2
  authentication_on sk2

end goal
```

```
environment()
```

References