Contents

1 question1 Theory

Built: 05 September 2019
Parent Theories: cipher, string

1.1 Theorems

[question1Thm]

```
⊢ ∀ signature.
     signVerify (pubK TrueSignatures) signature
       (SOME “pubK GoodBooks”) ⇔
     (signature =
      sign (privK TrueSignatures)
        (hash (SOME “pubK GoodBooks”)))
```

2 question2 Theory

Built: 05 September 2019
Parent Theories: aclDrules

2.1 Datatypes

```
commands = pay | debit

keyPrinc = Staff people | Role roles | Ap num

people = Alice | Bob

principals = PR keyPrinc | Key keyPrinc

roles = payer | payee
```

2.2 Theorems

[question2Thm]

```
⊢ (M,Oi,Os) sat Name (PR (Role payer)) controls prop pay ⇒
  (M,Oi,Os) sat
  reps (Name (PR (Staff Alice))) (Name (PR (Role payer)))
    (prop pay) ⇒
  (M,Oi,Os) sat
  Name (Key (Staff Alice)) quoting Name (PR (Role payer)) says
  prop pay ⇒
```

```
(M,Oi,Os) sat prop pay impf prop debit ⇒
(M,Oi,Os) sat
Name (Key (Role payee)) speaks_for Name (PR (Role payee)) ⇒
(M,Oi,Os) sat
Name (Key (Role payee)) says
Name (Key (Staff Alice)) speaks_for Name (PR (Staff Alice)) ⇒
(M,Oi,Os) sat
Name (PR (Role payee)) controls
Name (Key (Staff Alice)) speaks_for Name (PR (Staff Alice)) ⇒
(M,Oi,Os) sat
Name (Key (Staff Bob)) quoting Name (PR (Role Operator)) says
prop debit
```

Index