Information technology - Open Systems Interconnection - The Directory - Part 8: Authentication framework ISO/IEC 9594-8

There are two levels of authentication:

- simple authentication, using a password as a verification of claimed identity; and
- strong authentication, involving credentials formed using cryptographic techniques.

While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services.

- Unilateral authentication means that only one of the two entities is authenticated by use of the mechanism.
- Mutual authentication means that the two communicating entities are authenticated to each other by use of the mechanism.

```
certificate ::= SIGNED SEQUENCE  (
   version   [0] Version DEFAULT v1988,
   serialNumber   CertificateSerialNumber  ::=  INTEGER,
   signature  AlgorithmIdentifier,
   issuer   Name,
   validity   Validity  ::=  SEQUENCE  (
      notBefore   UTCTime,
      notAfter   UTCTime)
   subject   Name,
   subjectPublicKeyInfo  SubjectPublicKeyInfo ::= SEQUENCE  (
      algorithm   AlgorithmIdentifier,
     subjectPublicKey  BIT STRING))
```

- Entity authentication mechanisms allow the verification, of an entity's claimed identity, by another entity.
- An impersonator may reply, at a later date, a valid authentication exchange (this is a forfm of masquerade). To prevent such a reply, a time variant parameter, such as a time stamp, a sequence number, or a challenge may be used.
- Generally, for authentication purposes, the entities generate and exchange standardized messages. called tokens.
- Unilateral authentication provides one entity with assurance of the other's identity but not vice versa.
- Mutual authentication provides both entities with assurance of each other's identity.
- The trusted party is trusted by both entities.
- Both entities shall use a common set of data cryptographic techniques and parameters.
- During the operational life of a key, the values of all time variant parameters shall be unique.
- The distinguishing identifiers of the authenticating entities are already available or have been delivered by some other means.

An entity to be authenticated corroborates its identity by demostrating its knowledge of:

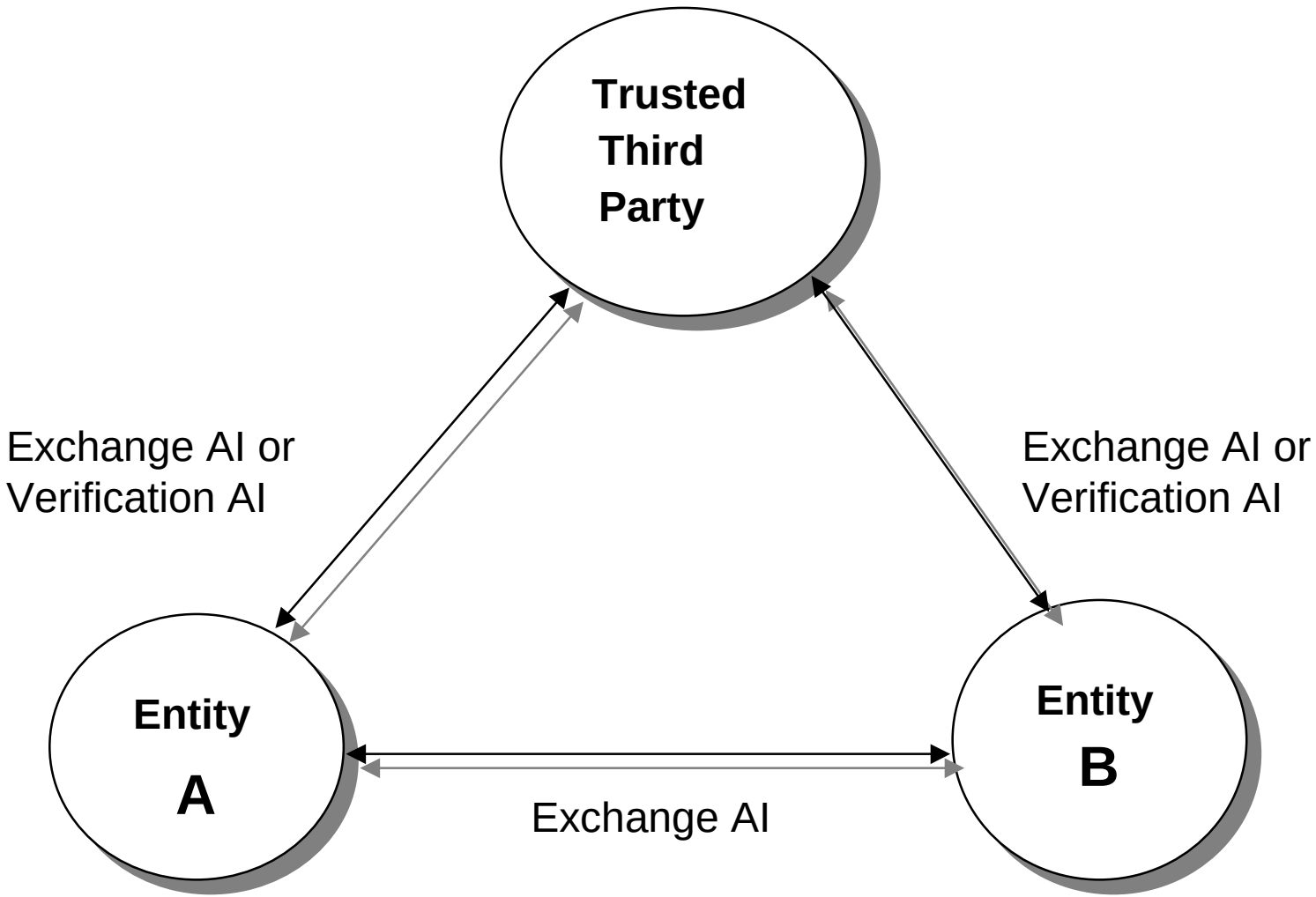
- part 2: a secret authentication key. This is achieved by the entity using its secret key to encipher specific data. The enciphered data can be deciphered by anyone sharing the entity's secret authentication key.
- part 3: its secret signature key. This is achieved by the entity using its secret signature key to sign specific data. The signature can be verified by anyone using the entity's public verification key.
- part 4: a secret authentication key. This is achieved by the entity using its secret key with a cryptographic check function applied to specific data to obtain a cryptographic check value. The cryptographic check value can be checked by anyone knowing the entity's secret authentication key who can recalculated the cryptographic check value and compare it with the value received.

The authentication mechanisms have the following requirements. If any one of these is not met then the authentication process may be compromised or it cannot be implemented.

- Part 2:
  - A claimant authenticating itself to a verifier shares a common secret authentication key with that verifier, or each entity shares a secret authentication key with a common trusted third party. Such keys shall be known to the involved parties prior to the commencement of any particular run of an authentication machanism.
  - If a trusted third party is involved it is trusted by both the claimant and the verifier.
  - The secret authentication key shared by a claimant and a verified, or by an entity and a trusted third party, is known only to those two parties and, possibly, to other parties they both trust.
  - Either assumption 1 or assumption2 is met.
  - 1. The encipherment algorithm and mode of operation used shall provide the recipient with the means to detect forged or manipulated data.
  - 2. The integrity of the enciphered data shall be ensured by an independent data integrity mechanism.

- Part 3:
  - A verifier shall posses the valid public key of the claimant (certificate).
  - A claimant shall have a secret signsture key known and used only by itself.
- Part 4:
  - A claimant authenticating itself to a verifier shares a common secret authentication key with that verifier. This key shall be known to the involved entities prior to the commencement of any particular run of an authentication machanism.
  - The secret authentication key shared by a claimant and a verified, shall be known only to those two entities and, possibly, to other parties they both trust.
  - The cryptographic check function f which takes as input a secret key K and a string Z to produce $f_K(Z)$ shall satisfy the following properties:
    - for any K and Z it shall be computationally simple to compute $f_K(Z)$;
    - for any fixed K, and given no prior knowledge of K, it shall be computationally infeasible to find a new (X,Y) such that $f_K(X)=Y$, even given knowledge of (X_i,Y_i) such that $f_K(X_i)=Y_i$.
  - The strength of the mechanism is dependent on the key length and its secrecy, on the nature of the cryptographic check function, and on the length of the check value.

Entity Authentication mechanisms - Part 1
General model



Authentication model

Entity Authentication - Part 2
Mechanisms using symmetric encipherment algorithms

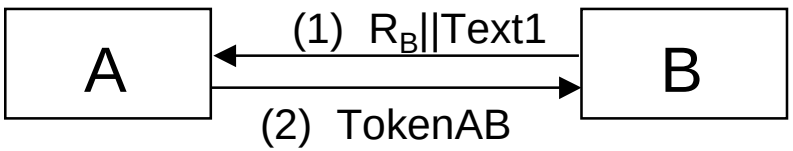
5 Mechanisms not involving a trusted third party

5.1 Unilateral authentication

5.1.1 One pass authentication

(2) $TokenAB = Text2||eK_{\mathbf{AB}}(\begin{smallmatrix}T_A\\N_A\end{smallmatrix}||B||Text1)$

5.1.2 Two pass authentication



(3) $TokenAB = Text3||eK_{\mathbf{AB}}(R_{\mathbf{B}}||B||Text2)$

5.2 Mutual authentication

5.2.1 Two pass authentication

(4)

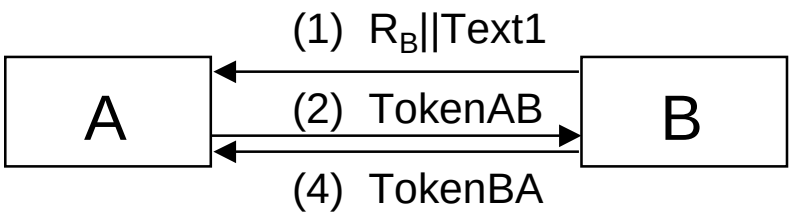
(2)

$TokenAB = Text2||eK_{\mathbf{AB}}(\begin{smallmatrix}T_A\\N_A\end{smallmatrix}||B||Text1)$

$TokenBA = Text4||eK_{\mathbf{AB}}(\begin{smallmatrix}T_B\\N_B\end{smallmatrix}||A||Text3)$

5.2.2 Three pass authentication

(5)



(3)

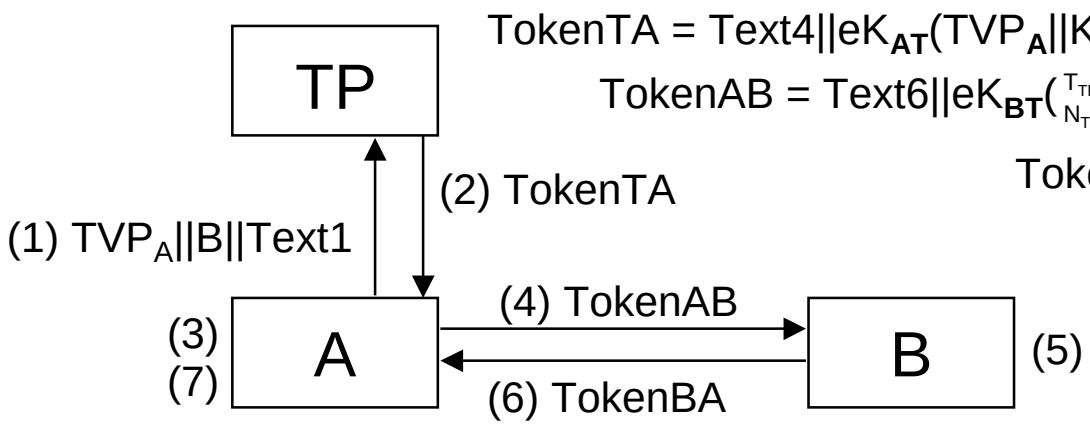
$TokenAB = Text3||eK_{\mathbf{AB}}(R_A||R_{\mathbf{B}}||B||Text2)$

$TokenBA = Text5||eK_{\mathbf{AB}}(R_B||R_A||Text4)$

Entity Authentication - Part 2
Mechanisms using symmetric encipherment algorithms

6 Mechanisms involving a trusted third party

6.1 Four pass authentication

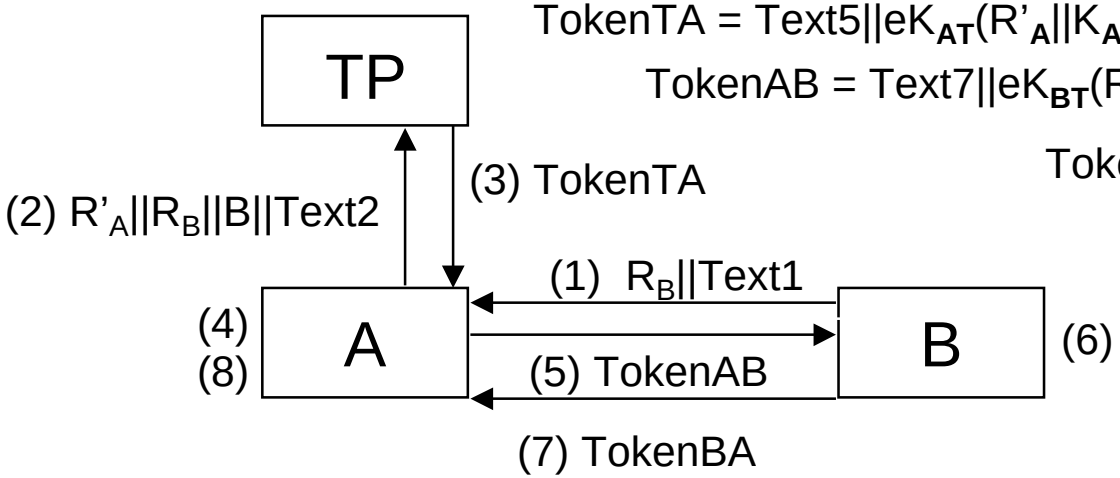


$TokenTA = Text4||eK_{AT}(TVP_A||K_{AB}||B||Text3)||eK_{BT}(\begin{smallmatrix}T_{TP}\\N_{TP}\end{smallmatrix}||K_{AB}||A||Text2)$

$TokenAB = Text6||eK_{BT}(\begin{smallmatrix}T_{TP}\\N_{TP}\end{smallmatrix}||K_{AB}||A||Text2)||eK_{AB}(\begin{smallmatrix}T_{A}\\N_{A}\end{smallmatrix}||B||Text5)$

$TokenBA = Text8||eK_{AB}(\begin{smallmatrix}T_{B}\\N_{B}\end{smallmatrix}||A||Text7)$

6.2 Five pass authentication



$TokenTA = Text5||eK_{AT}(R'_A||K_{AB}||B||Text4)||eK_{BT}(R_B||K_{AB}||A||Text3)$

$TokenAB = Text7||eK_{BT}(R_B||K_{AB}||A||Text3)||eK_{AB}(R_A||R_B||Text6)$

$TokenBA = Text9||eK_{AB}(R_B||R_A||Text8)$

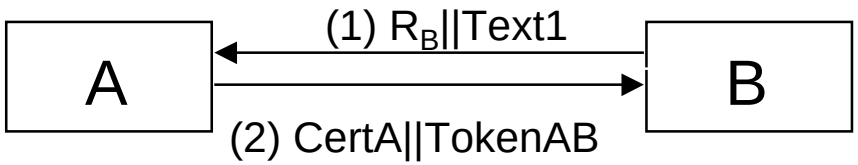
Entity Authentication - Part 3
Entity authentication using a public key algorithm

5.1 Unilateral authentication

5.1.1 One pass authentication

$$\text{TokenAB} = {}^{T_A}_{N_A}||B||\text{Text2}||s\mathbf{S_A}({}^{T_A}_{N_A}||B||\text{Text1})$$

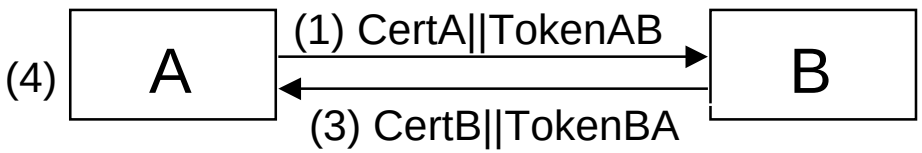
5.1.2 Two pass authentication



$$\text{TokenAB} = R_A||R_B||B||\text{Text3}||s\mathbf{S_A}(\mathbf{R_A||R_B}||B||\text{Text2})$$

5.2 Mutual authentication

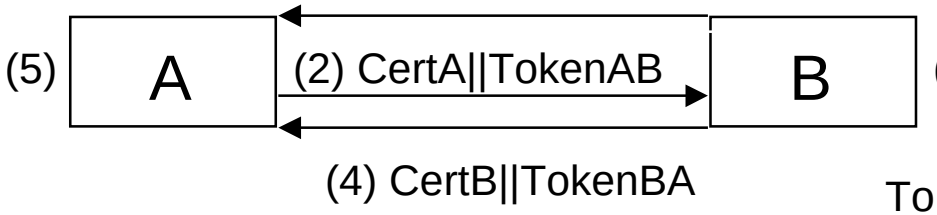
5.2.1 Two pass authentication



$$\text{TokenAB} = {}^{T_A}_{N_A}||B||\text{Text2}||sS_A({}^{T_A}_{N_A}||B||\text{Text1})$$

$$\text{TokenBA} = {}^{T_B}_{N_B}||A||\text{Text4}||sS_B({}^{T_B}_{N_B}||A||\text{Text3})$$

5.2.1 Three pass authentication



$$\text{TokenAB} = R_A||R_B||B||\text{Text3}||sS_A(R_A||R_B||B||\text{Text2})$$

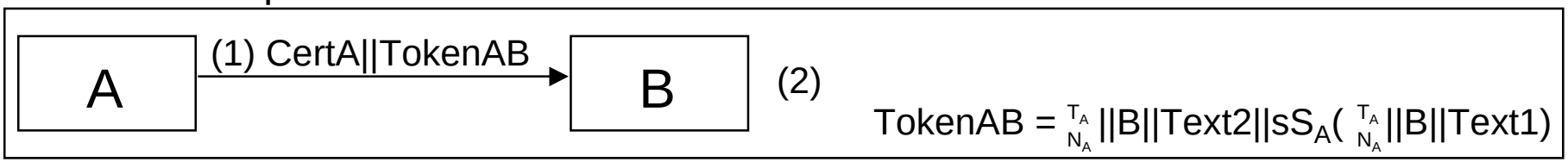
$$\text{TokenBA} = R_B||R_A||A||\text{Text5}||s\mathbf{S_B}(\mathbf{R_B||R_A}||A||\text{Text4})$$

Entity Authentication - Part 3

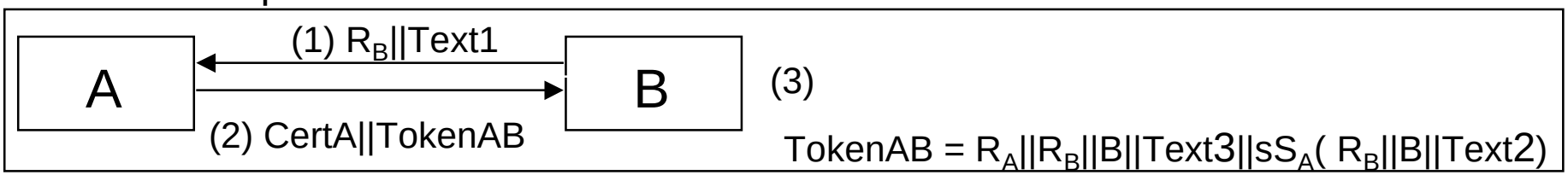
Entity authentication using a public key algorithm

5.1 Unilateral authentication

5.1.1 One pass authentication

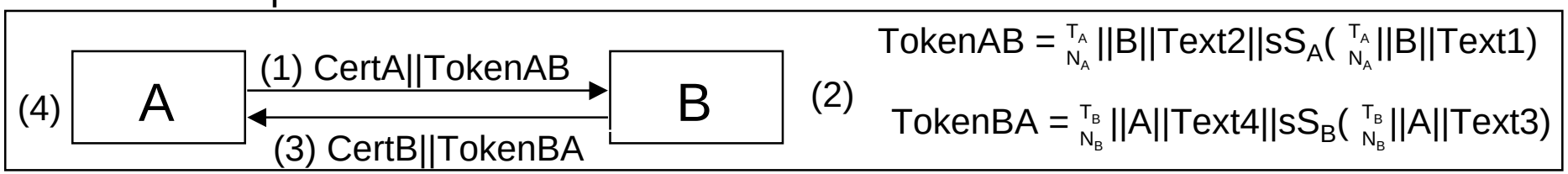


5.1.2 Two pass authentication

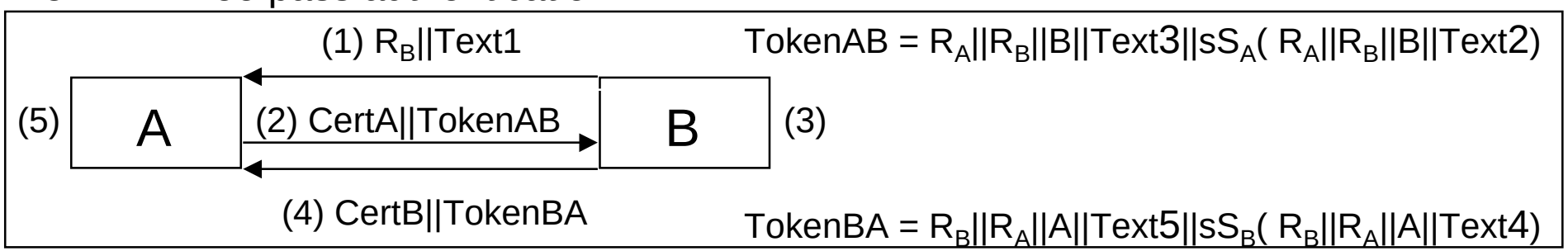


5.2 Mutual authentication

5.2.1 Two pass authentication



5.2.1 Three pass authentication



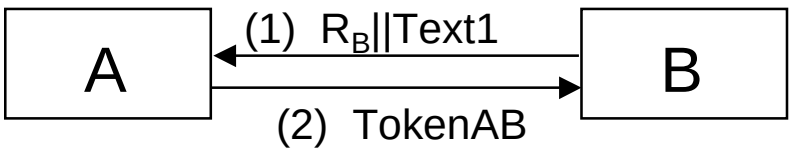
Entity Authentication - Part 4
Mechanisms using a cryptographic check function

5.1 Unilateral authentication

5.1.1 One pass authentication

(2) $\text{TokenAB} = {}^{T_A}_{N_A}||\text{Text2}||f_{\mathbf{K}_{AB}}({}^{T_A}_{N_A}||B||\text{Text1})$

5.1.2 Two pass authentication



(3) $\text{TokenAB} = \text{Text3}||\mathbf{f}_{\mathbf{K}_{AB}}(R_B||B||\text{Text2})$

5.2 Mutual authentication

5.2.1 Two pass authentication

(4)

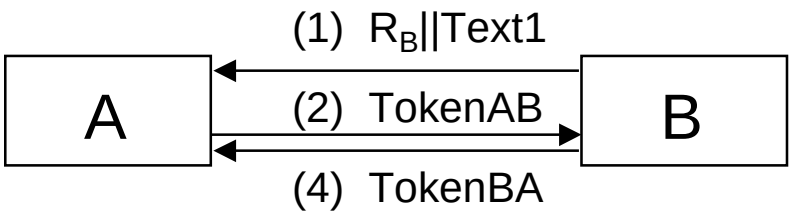
(2)

$\text{TokenAB} = {}^{T_A}_{N_A}||\text{Text2}||f_{\mathbf{K}_{AB}}({}^{T_A}_{N_A}||\mathbf{B}||\text{Text1})$

$\text{TokenBA} = {}^{T_B}_{N_B}||\text{Text4}||\mathbf{f}_{\mathbf{K}_{AB}}({}^{T_B}_{N_B}||\mathbf{A}||\text{Text3})$

5.2.1 Three pass authentication

(5)



(3)

$\text{TokenAB} = R_{\mathbf{A}}||\text{Text3}||\mathbf{f}_{\mathbf{K}_{AB}}(R_A||R_B||B||\text{Text2})$

$\text{TokenBA} = \text{Text5}||f_{\mathbf{K}_{AB}}(R_B||R_A||\text{Text4})$