Secure Token Concept within a Near Field Communication Ecosystem

FH OÖ Forschungs & Entwicklungs GmbH • Hagenberg • Linz • Steyr • Wels

NFC-Research Project

- Launch: Fall 2005
- Member of NFC Forum for Standardization
- Different Areas of Interests
  - Hardware Development
  - Use cases and Software/Application Development
  - Usability
  - Security
- NFC Trials on University Campus

Goal

- Standardize Ticketing/Access Solution for NFC Devices to allow secure transactions
  - Definition of an Infrastructure/Participants
  - Secure Protocol whole ticketing flow
- Integration of NFC Ticketing Software into the Operating System of mobile Devices

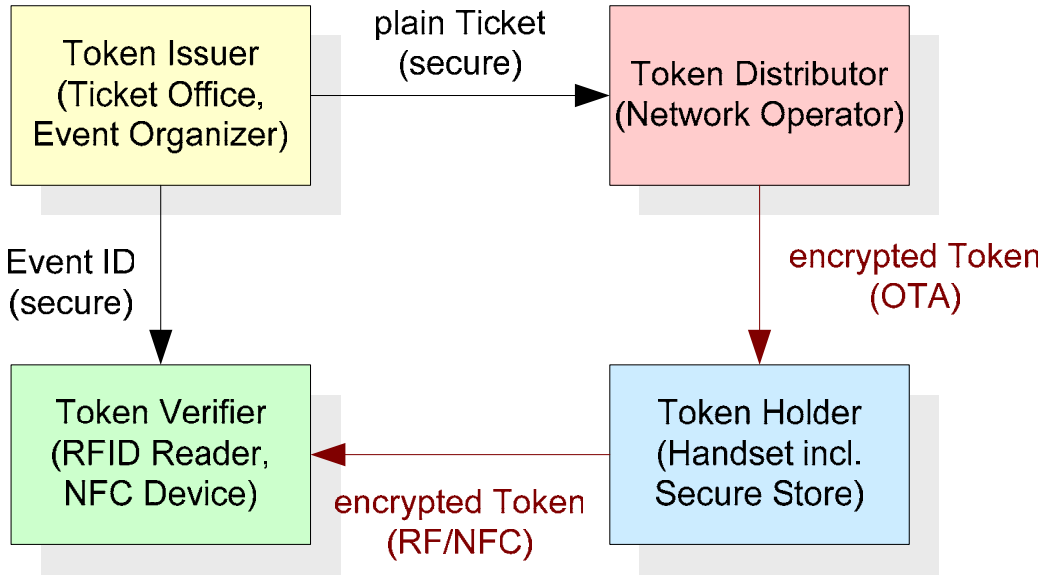
Requirements

- Target Platform: Mobile Phone
- Token Delivery via SMS/WAP Push (~ MMS)
- Secure Communication from Ticket Issuer to Access Gate
- Multiple Tickets/Ticketing-Applications possible within one device
- Good Performance for En/Decryption
- No User interaction required at Gate or when Ticket is received

Idea

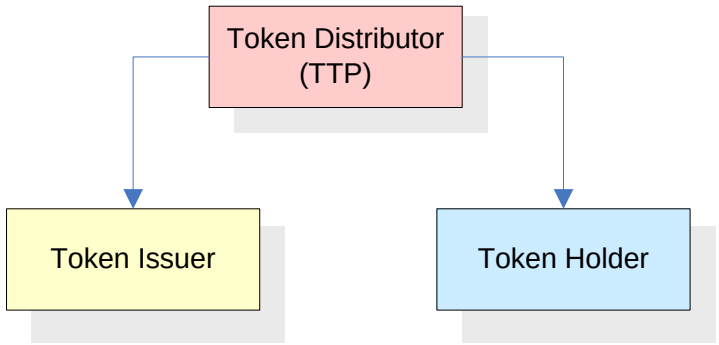
- Usage of Java Card Applet as Ticket Container
- Dynamic allocation of Tickets (not limited to Memory-Blocks)
- Secure-Element holder responsible for Applications on Java Card

Token Flow


Token Issuer
(Ticket Office,
Event Organizer)
plain Ticket
(secure)
Token Distributor
(Network Operator)
Event ID
(secure)
encrypted Token
(OTA)
Token Verifier
(RFID Reader,
NFC Device)
Token Holder
(Handset incl.
Secure Store)
encrypted Token
(RF/NFC)

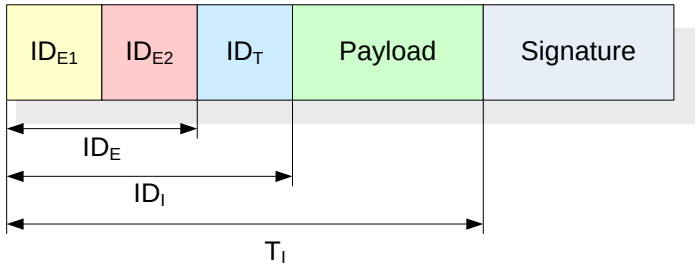
Participants

- *Token Distributor*: Trusted Third Party), signs public keys of other instances with its private key.
- *Token Holder*: Contains signed public Key; needed for secure Communication to Reader and Ticket Distributor
- *Token Issuer:* holds signed ID for each ticket/event; also needed for authentication to mobile phone. Signed public key needed for authentication against ticket distributor

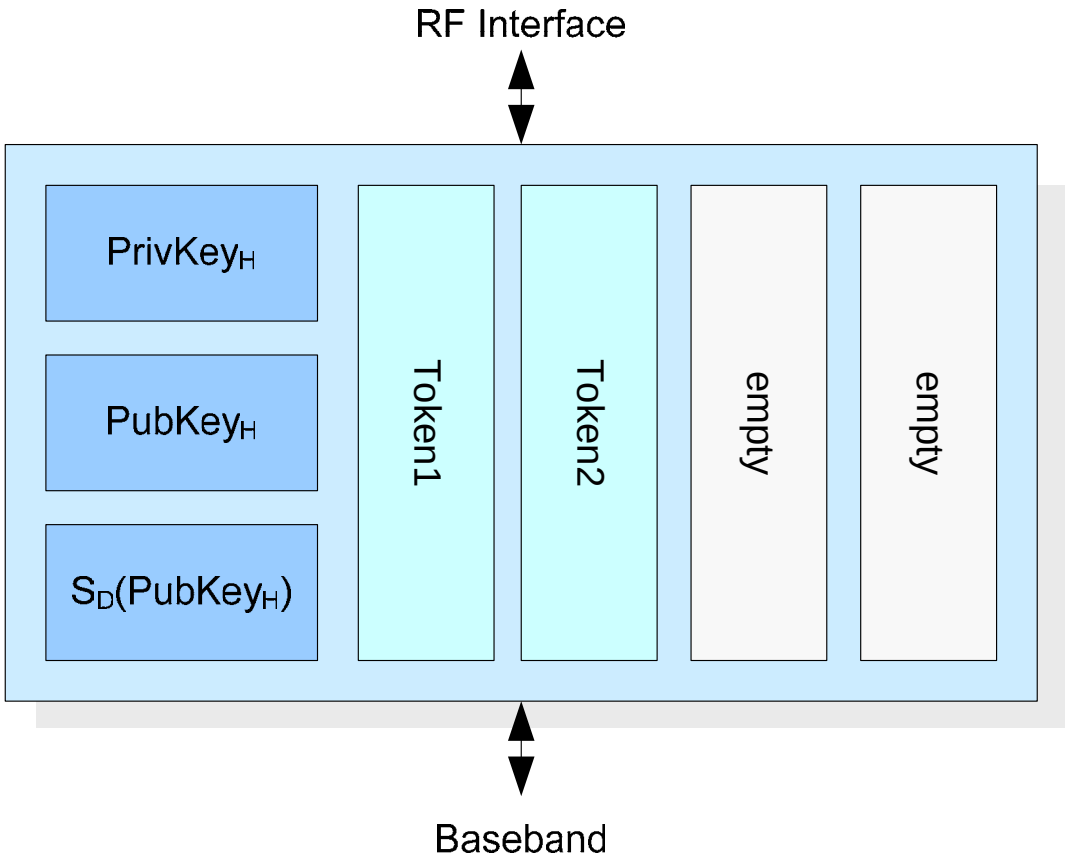


Token

- ID_E for Event (split between Issuer and Distributor; eg. 3 bytes + 5 bytes)
- ID_I for Token (eg. 8 Byte set by Token Issuer)
- Combination of ID_E and ID_I necessary for valid ticket.
- Payload (Counter, Name, Period of Validity, …)
- Signature



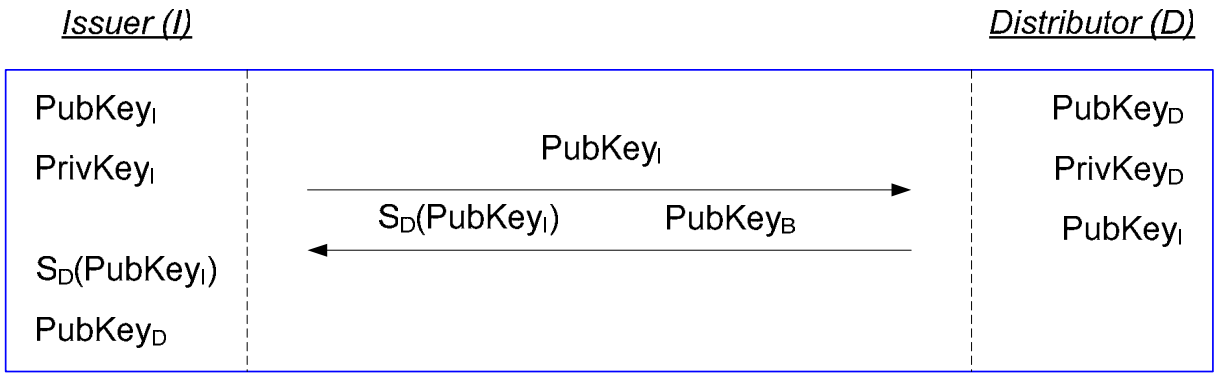
Secure Element



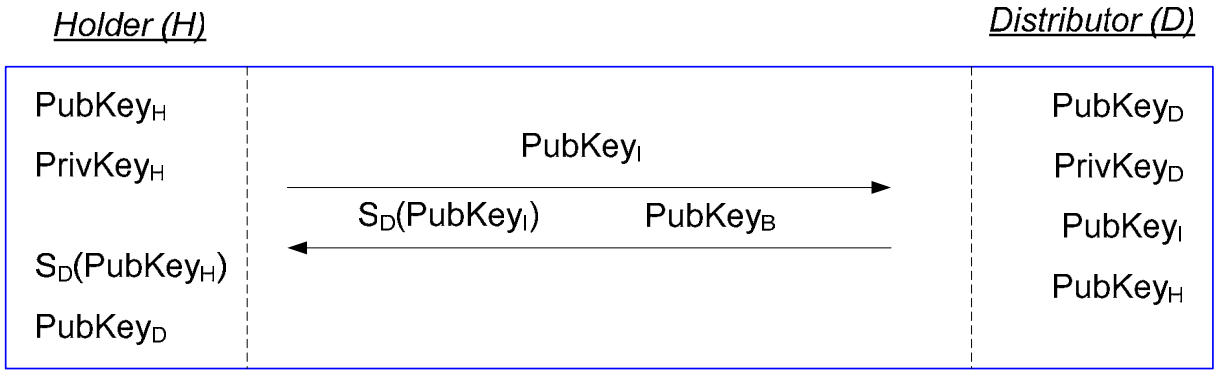
Protocol

- Key Exchange & Installation of Application
  - Certification of Token Issuer
  - Certification of Token Holder
- Preparation of Token
  - Request for Token ID
  - Initialization of Token Verifier
- Booking of Token
  - Transfer of Ticket from Organizer to Distributor
  - Delivery of Ticket to Token Holder
- Verification of Token

Key Exchange & Installation of Application

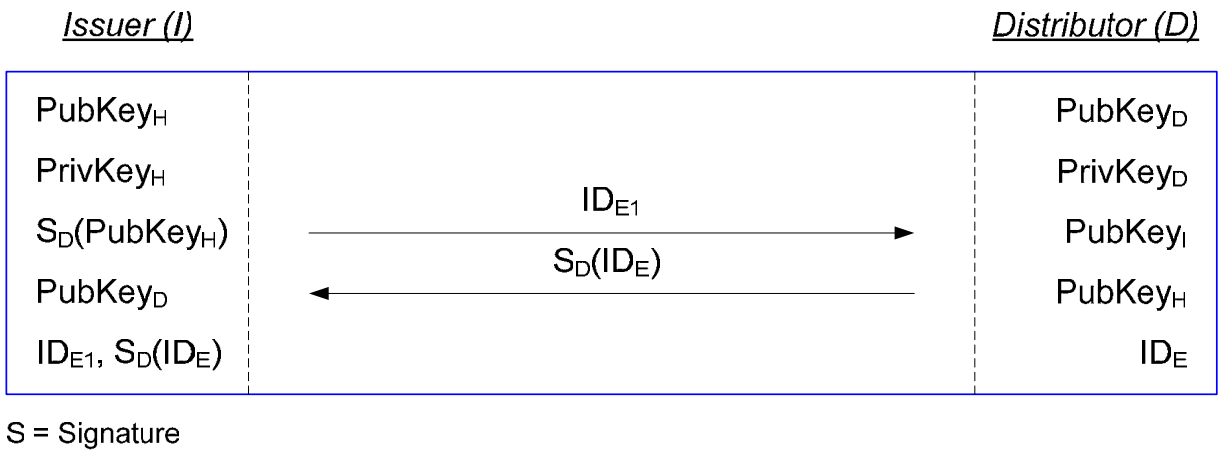


S = Signature



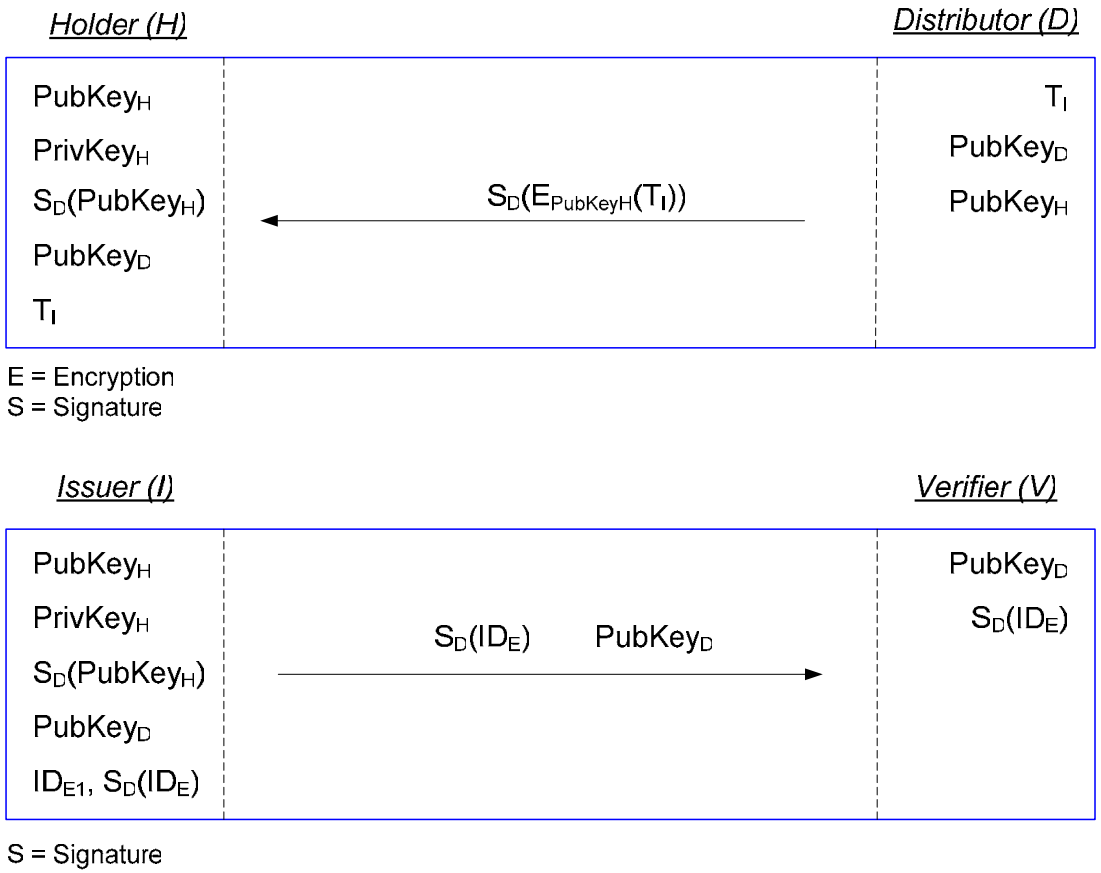
S = Signature

Preparation of Token

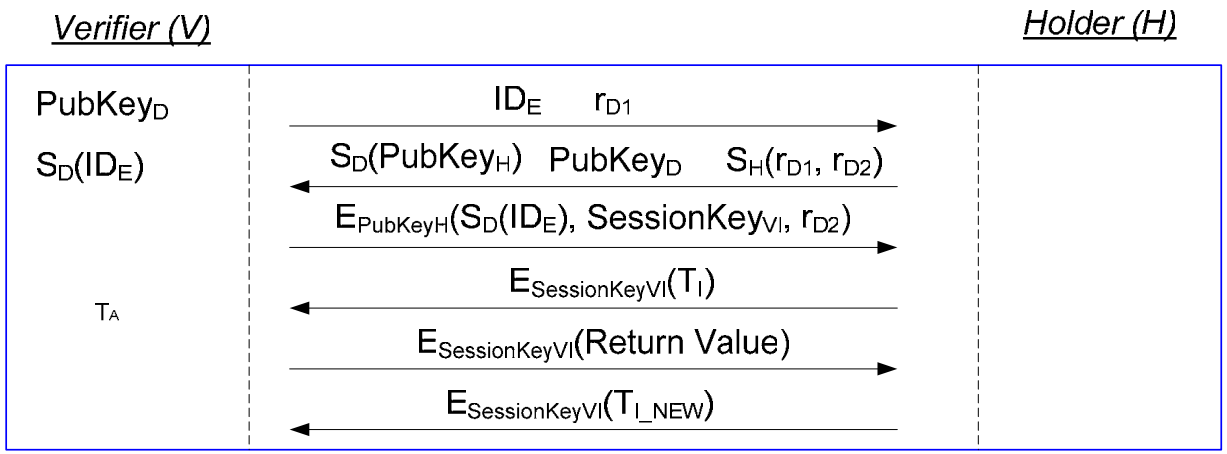


S = Signature

Booking of Token



Verification of Token



E = Encryption
S = Signature

Conclusion

- For Secure Ticketing a trusted Instance (“Distributor”) needs to be introduced.
- Owner of Secure Element needs to be defined.
- Ticket Container, Security Protocol and Token Format need to be defined.
- NFC Devices should be delivered with pre installed Ticket Management Software.