|  |  |
| --- | --- |
| Use Case | Remote identity proofing for online air flight check-in and using the derived credentials for airport services (e.g. boarding gate and the duty-free shop verifications) |
| Scope | Authentication and Identity Proofing based on Spanish eID |
| Preconditions | A) A DNIe 3.0 smart card issued by the Spanish administration (use of Card Access Number printed on its front is also mandatory)  B) A smart device (e.g. mobile phone) with NFC and camera  C) Client software capable of reading data from DNIe |
| Success end-condition | Passengers identity has been confirmed and, depending on the application, derived credential or claims are stored in mobile boarding pass and/or biometric feature is extracted for verification at the boarding gate |
| Primary and secondary actors | Passenger, airline company, airport operator |
| Trigger | i. Passenger (user) will open the ID proofing app  ii. The part of the mobile app is reading the DNIe 3.0 through NFC interface and it will ask the user for the Card Access Number (CAN), which is printed in the front of the card. Optionally, this CAN number can be stored in the app for user convenience.  iii. The end-user will be asked to bring the DNIe 3.0 document close to the NFC antenna of the NFC-enabled smart device (around 1 cm of distance is allowed).  iv. Using the CAN number, an encrypted Password Authenticated Connection Establishment (PACE) channel will be established between the document and the NFC-enabled device. If the (entered or selected) CAN number does not match the document the PACE channel will not be established and the user will be notified asking to enter again the number.  v. Once PACE encrypted secure channel is established a secured exchange of commands and responses will take place, allowing to read the public data from the eID document.  vi. optional step - if the user is requesting Enrolment in Airline eID ecosystem with a captured face image with the smart device (tablet, mobile phone) camera.  vii. optional step - Mobile app creates and stores documents or tokens (e.g. mobile boarding pass, derived claims such as “age > over 18” etc.) in protected user’s mobile wallet, that can be presented at the airport. It can also store additional information as part of transaction logs in the audit trail such as the link between the breeder document and derived token.  viii. As a final step, the wrapper can also provide the obtained attributes and facial image signed with the digital signature certificate of the user (SHA1 with RSA is used). From the user perspective, this will involve two more dialogues: a displaying of the attributes values to sign and the request for the user to enter his Personal Identification Number in order to be able to load from the card the digital signature certificate. DNIe allows user to make 3 attempts for entering this PIN, if he fails, the card will lock and it is only possible to unlock it at a Spanish police station presenting one of the 2 fingerprints enrolled when the card was originally issued. |
|  |  |
|  |  |