



CryptoBiometrics for Enhanced Trusted Identity Management: Dreams & Reality

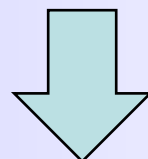
Increase security trust on secure areas

Odysseas Spyroglou,
3D SA General Aviation Applications, GR

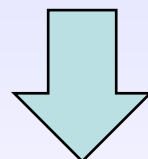
IdM & Security Trust

Identification Management : a means to security

Biometrics : a tool (?) for better IdM



IdM + Biometrics = Increased Security (and perception)



Increased Security Trust

Secure Areas & Airports

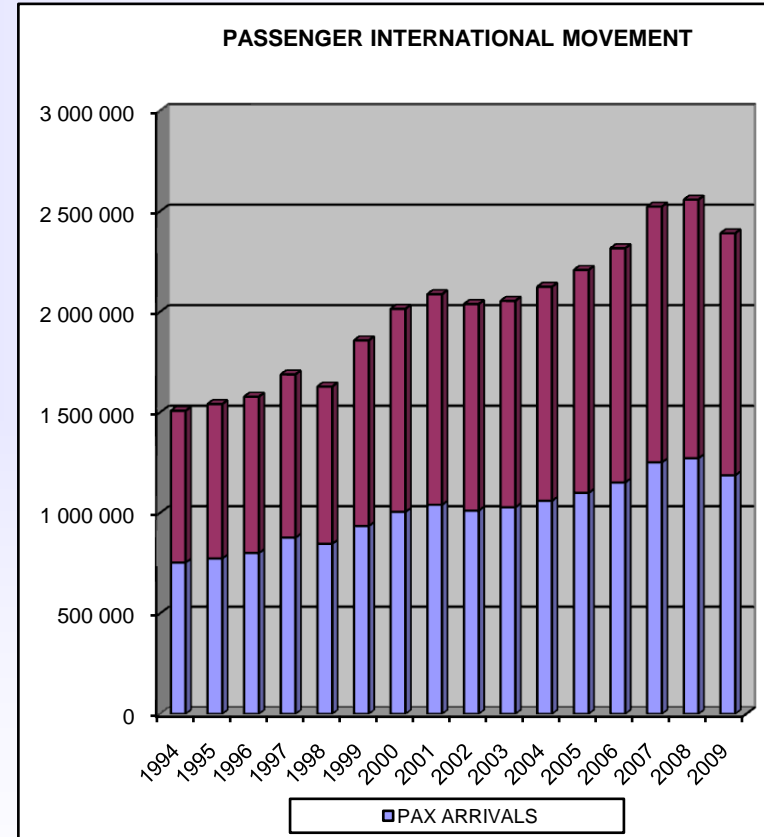
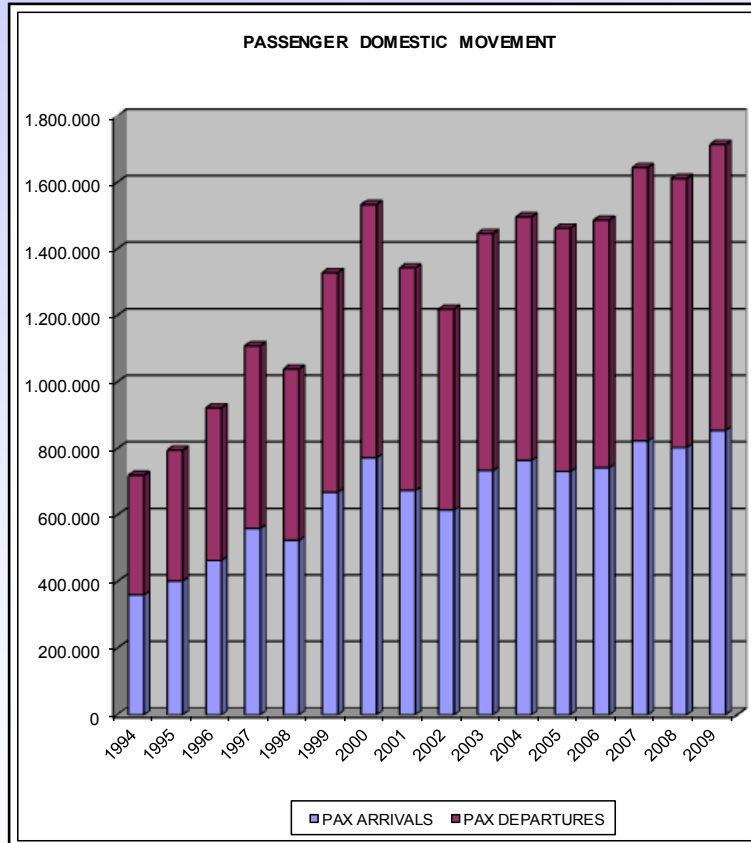
- Importance of security greatly increased after 9/11
- What is a secure area ?
- Critical Infrastructures: *assets that are essential for the functioning of a society and economy (hospitals, gov buildings, airports)*
 - European Programme for Critical Infrastructure Protection (EPCIP) EU COM(2006) 786 final
- Airport / aviation security
 - Regulation (EC) No 300/2008 on common rules in the field of civil aviation security
 - Commission Regulation (EU) No 185/2010 laying down detailed measures for the implementation of the common basic standards on aviation security

Zones and Levels of Trust

Security zone	Level of trust
Maneuvering area	very high
Air traffic control	very high
Airport ramp	high
Departures Terminal	high
Arrivals Terminal	medium
Customs	medium

Access Level	Level(s) of trust
Full Access	very high + high + medium
Full Access except for maneuvering area & air traffic control	high + medium
Airport ramp	high
Departures and Arrivals Terminals	high + medium
Arrivals Terminal	medium
Customs	medium

The case of the Thessaloniki Airport



The Thessaloniki Airport Demonstrator



Demonstrator applications

Pseudo Identity (User holds a card)

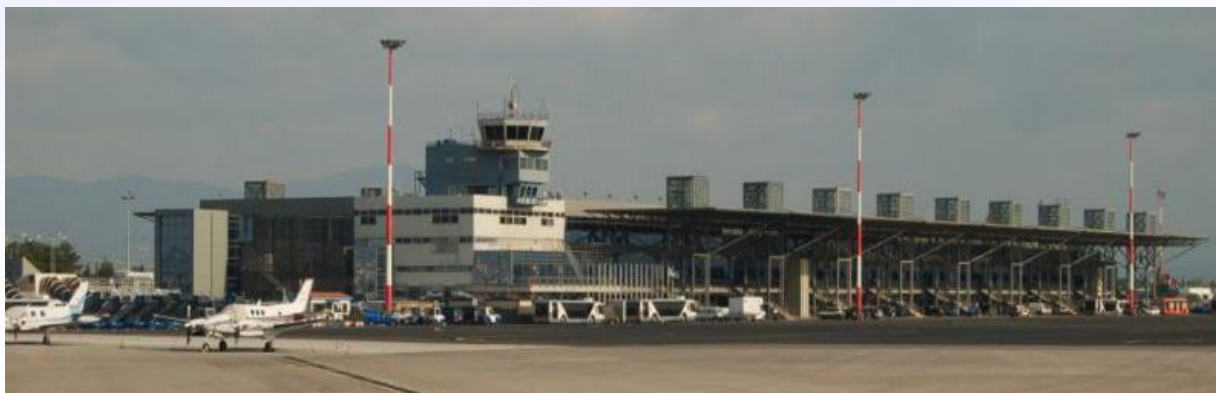
Staff Member Access to Security Zones

- multiple access rights

Secure Access Control (no smartcard for user)

Staff Member Access to Cargo Facility

- secure access control



Some data from the Trial at Thessaloniki Airport



Airport Demonstrator

- Participants: 30 Volunteers from 3DSA, Olympic Airways and HCAA
- One Enrolment Office – 4 trained screeners
- 3 Access Control Points for PI
- 1 Access Control Point for SAC
- 1,5 month of field trials
- Very Positive results

Demonstrator Functionalities

The functionalities examined by the demonstrator included the following:

1. Enrolment and verification
2. Duplicate enrolment checks, e.g.: a user can not enroll multiple times to the same service.
4. Revocation and re-enrolment, e.g.: a user revokes a pseudo-identity and requests a new enrolment to the same service.
5. Watch lists

Inform Consent & Data Privacy

- Extensive work and support of the project to the DPA
 - Letter: Accompanying Letter to HDPDA
 - Information Note: to explain the project and the demonstrator
 - Description of the organizational and technical security measures to ensure privacy and protection of sensitive data
 - Controller – Processor Agreement between 3DSA and the rest of the project Partners that would be able to access the data
 - Description of Confidentiality Obligation
 - Employee Consent Form
 - HPDA Form 1 & Appendix 1 & 2 regarding Notification of keeping sensitive data
- Continuous support and training to participants

Secure Access Control

- The “Secure Access Control” protocol is an *identification protocol*
- Application:
Physical access control to security zones, e.g. an airport runway
- A group of users is enrolled for runway access
- During enrollment, each member of the group presents his or her fingerprint
- For access request:
 - a user presents his fingerprint
 - the fresh fingerprint is cross-compared with those stored in a local database in the terminal
 - in case of success, the claimant is granted access
 - in case of failure to identify, access is denied



Operational Scenarios

1. How easy is the installation of the system?
2. How easy was the administration of the system (enrollments, revocations)?
3. The rate of False Acceptances and False Rejections.
4. Some operational scenarios that are important:
 - Lost Card. Intrusion attempt using a lost card
 - Security leak. Attempt of a registered owner to override his rights. User tries to access an area where he has no access rights.
 - Change of Access Rights to a Group: The rights of some users are revoked and new users are added.

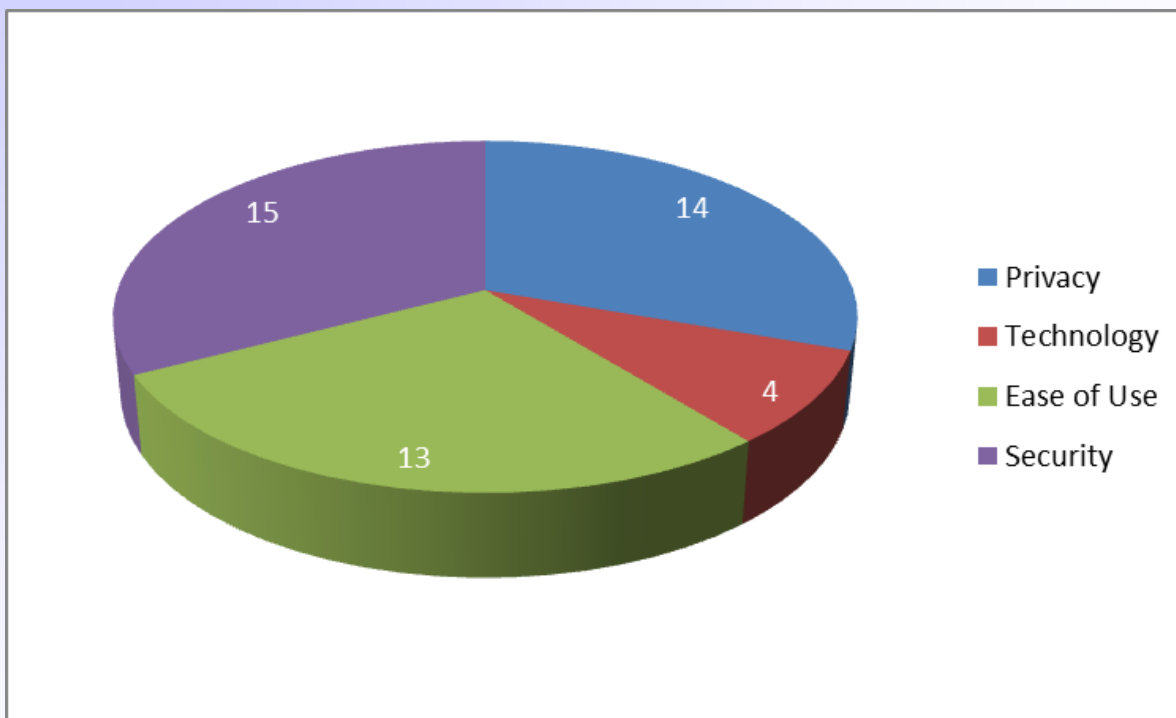
The system operated smoothly to all the above scenarios.



Questions to the participants

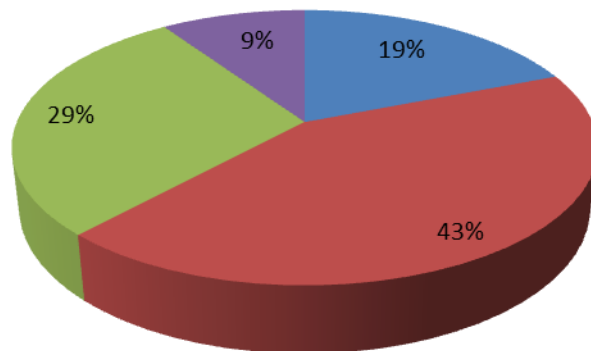
- Did you find the system easy to use (1 difficult – 5 very easy)?
- Did you find the system quick and responsive ?
- Did you find that the system was usually mistaken ?
- Were you feeling comfortable using it or not ?
- Were you feeling that your privacy was at risk ?
- Do you consider privacy aspects of the processing of your biometric data important ?
- Do you consider it important that biometric data are used in an application in a protected way (1 not important – 5 very important)?
- Would you agree on the operational use of the system in security applications (e.g. Access Control) (1 do not agree – 5 Agree)?
- Which one you consider the two most important aspects of the TURBINE system? A. Privacy B. Technology C. Ease of Use D.Security
- What other applications you believe the system would be useful in?

Most important aspect of TURBINE



Refuses to use the system

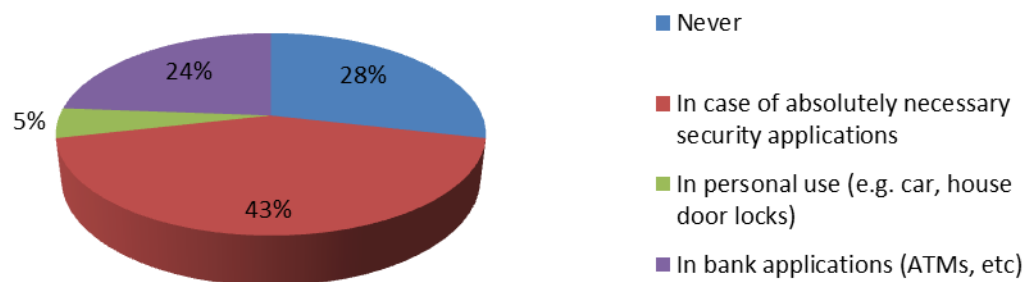
Why did you refuse to participate to the TURBINE demonstrator?



- I'm not obliged to.
- I don't want to give my biometric data to my boss.
- I don't want my entire day movements to be recorded.
- I don't trust the controller to secure my data.

Refuses to use the system

**Would you accept the use of such a system
and when?**





Conclusion

- A successful demonstrator with positive comments
- Real interest especially from security operators and screeners
- Importance of Privacy and Data protection

Thank you



- For more info :

Odysseas Spyroglou

R & D Advisor

3D General Aviation Applications S.A.

2 Skiathou st., 546 46 Thessaloniki Greece

Tel.: +30 2310 413585

email: ospyroglou@3dsa.gr, ospyroglou@gmail.com