

Traffic at airports and borders is increasing so dramatically that governments are looking for secure identification applications and cost-effective border crossing strategies. Oberthur Technologies is already producing e-passports compliant with the International Civil Aviation Organization (ICAO) standards for the use of contactless chips and biometric identification within travel documents.



ID-One™ ePass products from Oberthur Technologies are fully compliant with ICAO and EU-EAC specifications, guaranteeing interoperability worldwide and in Europe. They also fully comply with EU regulations since they are Common Criteria Certified for BAC and for EAC, with Active Authentication activated.

They are ready for Extended Access Control deployment for pilots starting now with the highest security levels, having achieved Common Criteria certification Protection Profile EAC with Active Authentication.

Oberthur Technologies is implicated in all security evaluations available on the market today and offers highly secure operating systems. Its organization reflects its desire for an optimized global strategy while staying close to its customers.

Field experience has demonstrated Oberthur Technologies success in deploying high-level contactless e-passports with the massive volume rollout of the electronic passport in Belgium.

Oberthur Technologies offers a complete range of products, solutions and services for travel documents: from operating systems, chips and inlays to epassport covers or finished e-passports (chip + antenna + booklet) with the corresponding personalization system and inspection systems software.

ID-One EPass

- Fully compliant to ICAO & EU specifications
- 1st ICAO e-passports deployment in November 2004
- E-passport application evaluated Common Criteria EAL 4+





Extended Access Control

ID-One ePass products are ready for Extended Access Control thus efficiently protecting access to highly sensitive personal data such as fingerprints and/or iris.

Features:

- RSA PKCS#1 V1.5 and RSA PSS with key length up to 1536 bits
- Elliptic Curves GF(p) with key length up to 512 bits
- SHA-1 and SHA-256 supported
- Extended Length supported
- 2 keys for Chip Authentication supported



Basic Access Control

- Ensures confidentiality of Identity
- Added feature to increase security: time for establishment of BAC increased in case of previous failed attempts



Active Authentication

Ensures that the passport is not a clone.



Passive Authentication

Ensures the authenticity of the passport's origin.



ID-One ePass products are fully compliant with ISO, ICAO and EU-EAC specifications. They undergo rigorous security and functionality evaluations.

ICAO operating system range and features

		Version	Free EEPROM (Kbytes)	ISO 14443 T=CL Type A	ISO 14443 T=CL Type B	Extended Length APDU*	Passive Authentication	Active Authentication	Basic Access Control	Extended Access Control	Max RSA key length (bits)	RSA key generator	EC DSA max key size (bits)**	EC Diffie-Helman	SHA-1	SHA-256	Common Criteria Certification EAL4+ PP BAC with AA	Common Criteria Certification EAL4+ PP EAC RSA	Common Criteria Certification EAL4+ PP EAC Elliptic Curves	Match-on-Card	
NATIVE	ID-One ePass 32	Source A v1.23 36	•	•	•	•	•	•	1024	•	•	•	•	•	•	•	•	•	•	•	
		Source B v1.23 36	•	•	•	•	•	•	1024	•	•	•	•	•	•	•	•	•	•	•	
	ID-One ePass 64	Source A v1.23 64	•	•	•	•	•	•	1024	•	•	•	•	•	•	•	•	•	•	•	•
		Source B v1.23 64	•	•	•	•	•	•	1024	•	•	•	•	•	•	•	•	•	•	•	•
		Source C v2.0 64	•	•	•	•	•	•	1536	•	384	•	•	•	•	•	•	•	•	•	•
	MULTI-APPLICATION	ID-One ePass J 32	Source A v1.32 32	•	•	•	•	•	•	1024	•	•	•	•	•	•	•	•	•	•	•
Source B v1.32 32			•	•	•	•	•	•	1024	•	•	•	•	•	•	•	•	•	•	•	
ID-One ePass J 64		Source A v1.32 64	•	•	•	•	•	•	1024	•	•	•	•	•	•	•	•	•	•	•	•
		Source B v1.32 64	•	•	•	•	•	•	1024	•	•	•	•	•	•	•	•	•	•	•	•
		Source C v2.2 64	•	•	•	•	•	•	1536	•	512	•	•	•	•	•	•	•	•	•	•
ID-One ePass J 128		Source A v2.2 128	•	•	•	•	•	•	1536	•	512	•	•	•	•	•	•	•	•	•	•

*Extended Length APDU support as defined by ISO 7816 **Elliptic Curves DSA Gfp algorithm