Annex I: Minimum Technical Specifications and Security Features	
1.1. Minimum Physical Security Features	
Elements	Mandatory Features
i. Paper Substrates	– controlled UV response – two-tone watermark – chemical sensitizers – appropriate absorbency and surface characteristics – reactive inks and chemical sensitizers in paper
ii. Background and Text Printing	– two-colour guilloche background – rainbow printing – microprinted text – unique data page design – offset/intaglio printing techniques for static data
iii. Inks	– UV florescent ink – reactive inksign – ink with optically variable properties
iv. Numbering	– page numbering on all visa pages – printed and/or laser-perforated passport number
v. Protection against photo substitution and alteration	– integrated biographical data – security background merged within portrait area – visible security device overlapping portrait area – heat-sealed secure laminate or equivalent – additional photo (ghost photo/ultra violet) – DOVID/ hologram
vi. Protection against page substitution	– secure sewing technology – UV fluorescent sewing thread – unique data page design – page numbers integrated into security design – multi-color sewing thread
1.2 Protection against Theft and Abuse	
- **good physical security** - **full audit trail** - **serial numbers on blank documents, as applicable** - **tracking and control numbers of components, as applicable** - **secure transport of blank documents** - **international information exchange on lost and stolen documents (INTERPOL)** - **internal fraud protection procedures** - **security vetting of staff** - **CCTV in production areas** - **centralized storage and personalization, where possible**	
1.3 Electronic Security Features	
i. Location of	- either back cover of passport or bio data page

	chip	(polycarbonate)
ii.	**Minimum size of chip**	- 32 kilobytes
iii.	**Biometrics**	- Electronic/digital photo (facial image) – minimum size as per ICAO standards - Fingerprint (number of digits stored subject to national laws and regulations) - signature
iv.	**Electronic Security Mechanisms**	- passive authentication - active authentication - BAC and PACE access control - extended access control
1.4 Public Key Directory (PKD)		
All Member States are recommended to implement and join the public key directory.		

NOTE:
The above-mentioned are the adopted minimum security features. Member States have the discretion to add other features as they deem necessary.