Requirements for the new generation of Georgian identity documents

1 INTRODUCTION

When “passport” or “ePassport” is stated in the present document without explicitly specifying document type, the corresponding requirement applies to all documents with type of “TD-3” given in table #1. Similarly, when “eID card” is stated in the present document without explicitly specifying document type, the corresponding requirement applies to all documents with type “TD-1” given in table #1.

Table #1

No.	Name of object of purchase	Format	Quantity	Comments
1	Blank of biometric passport of citizen of Georgia	TD-3	2 400 000	
1.1	Specimen of Blank of biometric passport of citizen of Georgia	TD-3	2000	
2	Blank of biometric diplomatic passport of citizen of Georgia	TD-3	7000	
2.1	Specimen of Blank of biometric diplomatic passport of citizen of Georgia	TD-3	1000	
3	Blank of biometric service passport of citizen of Georgia	TD-3	7000	
3.1	Specimen of Blank of biometric service passport of citizen of Georgia	TD-3	1000	
4	Blank of biometric travel passport of stateless person holding a status in Georgia	TD-3	7000	
4.1	Specimen of Blank of biometric travel passport of stateless	TD-3	1000	

	person holding a status in Georgia			
5	Blank of biometric travel document of refugee	TD-3	7000	
5.1	Specimen of Blank of biometric travel document of refugee	TD-3	1000	
6	Blank of neutral travel document	TD-3	7000	
6.1	Specimen of Blank of neutral travel document	TD-3	1000	
7	Blank of biometric travel document of person holding a humanitarian status	TD-3	7000	
7.1	Specimen of Blank of biometric travel document of person holding a humanitarian status	TD-3	1000	
8	Blank of compatriot card (form ID1)	TD-1	6500	
8.1	Specimen of blank of compatriot card (form ID1)	TD-1	1000	
9	Blank eID card (form ID1)	TD-1	3 500 000	
9.1	Specimen of blank eID card (form ID1)	TD-1	2000	
10	Blank temporary residence electronic card (form ID1)	TD-1	150 000	
10.1	Specimen of blank temporary residence electronic card (form ID1)	TD-1	1000	
11	Blank permanent residence electronic card (form ID1)	TD-1	30 000	

11.1	Specimen of blank permanent residence electronic card (form ID1)	TD-1	1000	
12	Blank neutral ID card Georgian-Ossetian (form ID1)	TD-1	7000	
12.1	Specimen of blank neutral ID card Georgian-Ossetian (form ID1)	TD-1	1000	
13	Blank neutral ID card Georgian-Abkhazian (form ID1)	TD-1	7000	
13.1	Specimen of blank neutral ID card Georgian-Abkhazian (form ID1)	TD-1	1000	
14	Blank temporary identification card (form ID1)	TD-1	7000	
14.1	Specimen of blank temporary identification card (form ID1)	TD-1	1000	

1.1 Definitions and use of terminology

1. **Equivalent standard** – Equivalence shall be defined according to the Georgian legislation (including Product Safety and Free Movement Code). During the first use of the standard as an "equivalent standard", PSDA shall be supplied with the references to relevant provisions of the Georgian legislation which would prove the equivalence of the standard (e.g. if the equivalent standard is used in the bid, the Bidder shall include the references in the tender proposal)
2. **Newer standard** - The new standard can be used only in case if it is issued by the same organization (in case of multi-organizations like ISO and IEC – at least one of them) and at least one of the following requirements are met: 1) it has the same number, or b) its text

explicitly states that the older standard is replaced with the new one. During the first use of the standard as a "newer standard", PSDA shall be supplied with the relevant excerpts from the newer standard as a proof (e.g. if the newer standard is used in the bid, the Bidder shall include the references in the tender proposal)

3. **Manufacturing site** - The site where the product (e.g. blank document) acquires its final form.

2 BIDDER INFORMATION

The Bidder shall fulfill requirements defined by the present document. The bidder has right to have related companies (see chapter 2.5) and subSuppliers.

The information and documentation required by this chapter and its sub-chapters shall be provided in the tender proposal.

2.1 PART 1: Financial capabilities

These requirements are regulated by the tender documentation_____

2.2 PART 2: Experience and references

These requirements are regulated by the tender documentation _____

2.3 PART 3: Technical and professional capabilities

1. Proposed document operating system(s), including eID, eMRTD and Auxiliary Data applications is/are developed by the Bidder, its related company, or subSupplier (name of the entity must be on the Common Criteria certificate). The Bidder shall be responsible for ensuring security of the product, promptly informing PSDA about possible and confirmed vulnerabilities in the products used, and supply of necessary software fixes of said vulnerabilities to PSDA without undue delay.
2. The Bidder takes responsibility to develop a risk analysis and a risk management plan which stipulates addressing of Project related risks, as well as a business continuity plan in the *force major* situations to guarantee execution of the Contract is resumed (in case of the interruption) within the shortest time. Said documents shall be a subject of the permanent revision from the supplier's end and maintaining it in line with the existing reality, during full validity period of the contract. PSDA has right to verify fulfilment of the given requirement at any time, using the any method it prefers, including the methods stipulated in the chapter 4.8 of the present document.
3. Proposed chip manufacturer must have integrated its chip products with at least 3 different identity and travel document operating system and application developers (vendors) and have at least 20 Common Criteria (EAL 5+ or higher) certificates listed on its name (where used as a platform for identity or travel document OS and applications). Certificates shall be included in the bid.
4. By placing the Bid, the Bidder acknowledges it is familiar with the Law of Georgia On the Forms of Strict registration https://matsne.gov.ge/en/document/view/30946 and takes responsibility to fully comply to the requirements of the mentioned law in case of the contract signature, during whole time of the contract validity (including amendments of the law).
5. All other requirements about the technical and professional capabilities are regulated by the tender documentation.

2.4 PART 4: Details of the offered blanks and other components

These requirements are regulated by the tender documentation_____

2.5 PART 5: Companies related to bidder

1. The bidder is entitled to rely on the experience of related companies and to present to this effect documents issued to related company/companies in confirmation of the admissibility criteria as defined in this document.
2. The Bid shall be appended with the consent of each of those related companies on involvement in the project (the related company may be involved in the part of the project in which the Bidder does not have an experience as per Chapter 2, within the entire validity term of the contract) which are specified by or on whose parameters the Bidder counts. The related company may be as follows:
   2.1. Subsidiary company of the bidder;
   2.2. Branch of the bidder;
   2.3. Parent company of the bidder;
   2.4. Subsidiary company of the parent company of the bidder.
3. Documents proving the hierarchy provided in paragraph 2 and evidencing shareholding of each parent company in each subsidiary company shall be attached to the bid. If any parent company is not 100% shareholder of any subsidiary company, report of one of the Big Four accounting firms (PricewaterhouseCoopers, Deloitte Touche Tohmatsu, Ernst & Young, KPMG) clearly specifying that parent company has controlling interest in subsidiary company shall also be attached to the bid.
4. If subsidiary company of parent company of the bidder is presented as related company, the parent company shall satisfy all the requirements for related company with regard to both subsidiaries (bidder and related company) as provided for by paragraph 3 of this Part – whether or not the parent company is presented as related company in the bid.
5. The documents presented in compliance with paragraph 4 shall confirm 100% shareholding and/or holding controlling interest in case of each parent-subsidiary company over 6 consecutive months till the moment of announcement of the bid.
6. In the scope of the present tender, only the companies about which the information is provided in the bid in full compliance with the requirements of the present chapter, will be considered as related companies. No other companies, regardless of their legal relationship with the Bidder, will be considered or evaluated.

3 CONTRACT EXECUTION

3.1 General requirements for project management and cooperation with the PSDA

1. Kick-off meeting shall be held after signing of the contract. The Supplier's personnel (to be used for execution of the Contract) namely Project and Sub-Project Managers (e.g. for blank document production, embedded electronics, middleware and systems) Blank Document Designer, System Architect and Lead developers shall be introduced to PSDA.

2. During the kick-off meeting the high level project plan shall be clarified

3. PSDA must have at least 10 (ten) working days (excl. official holidays in Georgia) for acceptance or rejection of goods and services in the scope of the present purchase.

4. During execution of the Contract the Supplier must ensure regular communication with PSDA.

5. The Supplier's Project Manager shall once a week submit to the PSDA's Project Manager status reports in line with the selected project management methodology agreed with the PSDA.

6. Project steering committee shall be established, containing project managers from both sides, high level representatives (CEOs and/or Chairmen, their deputies, etc.). The steering committee shall oversee project execution.

7. Upon PSDA's request, the Supplier shall establish local branch office in Georgia.

3.2 Contract steps and milestones

1. The Supplier shall no later than 6 (six) months after concluding the Contract deliver to the PSDA at least one set of the personalization equipment needed to produce electronic passport, the hardware for development and testing of extensions of personalization machines, as well as off-machine quality control library – by no later than 3 (three) months after contract signing. All personalization equipment stated in the present document shall be delivered no later than 7 (seven) months after concluding the Contract.

2. The Supplier shall no later than 6 (six) months after concluding the Contract deliver to the PSDA 500 (five hundred) test blanks for ePassport and 500 (five hundred) test blanks for eID card, which can be used for initial testing of the personalization solution. Test blanks are delivered free of charge.

3. The Supplier shall deliver to the PSDA copies of security certificates of the embedded software of the eID card and ePassport (IAS and eMRTD applications) no later than 14 (fourteen) months after conclusion of the Contract. These security certificates shall be issued by a security certification body member of SOG-IS agreement (www.sogis.org).

4. The Supplier shall deliver to the PSDA functional test reports of the embedded software proposed for eID card and ePassport obtained using a testing tool from a well-recognized test suite editor. Test for ePassport shall be delivered no later than 6 (six) months and for eID card no later than 10 (ten) months after conclusion of the Contract.

5. No later than 6 (six) months after conclusion of the Contract middleware of eID card (according to the chapter 4.7) shall be delivered to PSDA.

6. The Supplier shall deliver blank documents according to the delivery schedule given in the attachment.

7. The Supplier shall get approval of the purchaser for all blank design within 3 (three) months after the contract is signed (the purchaser's representative will be remotely available for the supplier during working hours (Georgian time) from the second day after the contract is signed). The purchaser's representative shall provide the supplier with the response for the issues sent by the supplier for approval within 3 (three) working days and total number of delayed days elapsed after the three-day period will be added to the above said 3-month term. The purchaser shall be responsible for approval of final design of the blank documents to be supplied and making of changes to relevant normative acts in connection with approval of final design of blank documents in compliance with the Georgian legislation. The supplier shall bear liability for any claims of third parties regarding infringement of copyrights related to security elements of the blank documents approved by the purchaser (except design elements offered by the PSDA itself).

8. The Supplier shall prepare one security design sample per document type for all passports and ID cards given in Table #1 and send them to the purchaser for registration in the Ministry of Finance within 1 (one) month after PSDA notifies the Supplier about approval of relevant normative act (order of the Minister of Justice of Georgia on approval of blanks) envisaged by this document.

9. The Supplier shall prove its ability of producing the blanks with the quality meeting requirements of the present tender (chapter 4.2 of the present document). The proofs, corresponding to the requirements of the chapter 4.2 shall be delivered to PSDA by no later than 1 (one) months after delivery of the blanks delivered according to the paragraph 8 of the present chapter. Normal usage conditions of the respective documents shall be delivered in the same time.

10. The purchaser is responsible for the registration of document blanks and get their registration identifiers within 2 (two) weeks after receiving samples for registration. Once these identifiers are provided to the Supplier, the Supplier is responsible to print documents of TD-3 format marked as "Specimen" in Table #1 in quantities given in the same table and deliver them to the Purchaser within 2 weeks. Documents shall contain registration identifiers provided by the Purchaser.

11. Algorithm and software modules for automated authentication of the document holder's facial image (according to the requirements of chapter 4.4 paragraph 5 of the present document) shall be delivered to PSDA not later than 6 (months) after signing the Contract.

12. By no later than 24 (twenty four) months after contract signature, the Supplier shall start delivering eID cards with Auxiliary Data Application deployed on them. If this results change of the IAS Application (e.g. because of inclusion of Single Sign On capability), the relevant certificate shall be delivered no later than the cards with the new IAS Application. The security certificate shall be issued by a security certification body member of SOG-IS agreement (www.sogis.org).

13. The Supplier shall supply to PSDA without any additional expenses and costs at least 10 (ten) sets of the special tools for examination of the level 2 security features of the blanks, where single set is consists of the one or many devices, which summarily allow to examine all features. The delivery shall be done no later than 1 (one) month before the first delivery of the object of purchase (blanks).

14. Failure of meeting the deadlines set in the present chapter will be a subject of penalties stipulated by the contract.

4 TECHNICAL REQUIREMENTS

4.1 General requirements

1. Blank eID cards and ePassport data pages (except hinge) must be made of 100% polycarbonate allowing to use laser engraving technology for their personalization purposes to be done in three personalisation sites of PSDA in Georgia using the personalization system developed by the purchaser.

2. Security features and methods for which high quality counterfeits have been detected, must not be used in the personalised documents.

3. During development of security features for the blanks and their pre-press processes, widely accessible standard software tools may be only used in the early stages of the development. In the final stage of the development of the security features and pre-press processes they shall be supplemented or replaced with the specialized tools with limited accessibility
4. Security features proposed for blank documents shall be arranged so that various elements supplement and are integrated with each other, and at the same time do not prevent checking each individual element separately.

5. The offered technologies shall ensure long-term protection against threats caused by increased accessibility to personalization equipment including laser engraving devices (larger supply, lower price, lack of restrictions for their acquisition).

6. The contract shall assume all associated costs of one-time upgrade of visual design and security features for each type of the documents, provided that existing security features will be replaced with new features with protection strength is not less than protection strength of the security features used before the upgrade was in the time of contract signature. PSDA must notify the supplier at least 1 (one) year before the scheduled launch time for the upgraded documents.

7. In case of concluding the contract, the Supplier may not refer during the contract execution to limitations of the technologies to be used, for example, tolerance, dimensions, available colour spectrum etc. which were not mentioned in the technical proposal during bidding.

8. No later than 6 (six) months after contract expiration, as well as no later than 6 months after upgrade according to paragraph 6 of the present chapter, all printing plates, lamination plates and other project specific materials required for production of the blanks shall be destroyed under PSDA's supervision. This requirement also applies to old project specific materials in case of the upgrade according to the paragraph 6 of the present chapter.

4.2 Durability Requirements

1. ePassport booklets shall be designed for at least 10 years life span. To meet this requirement, the test on sufficient number of booklets shall be conducted according to either one of the following (at least "Minimum level test plan" shall be passed with success):
   1.1. ICAO TR DURABILITY OF MACHINE READABLE PASSPORTS v3.2
   1.2. ISO/IEC 18745-1:2018 or newer.

2. eID card shall be designed to compliant with ISO/IEC 24789-1 with an ageing class 3, and usage class D. To meet this requirement, the test on sufficient number of cards shall be conducted according to ISO/IEC 24789-2.

3. The tests shall be conducted by the laboratory accredited according to ISO/IEC 17025. Laboratory accreditation certificate shall be provided and it shall list the relevant test methodology (ICAO TR, ISO/IEC 18745-1, ISO/IEC 24789-2 whichever is used) in the accreditation scope.

4. If the primary portrait personalization technology does not rely solely on the laser engraving and assumes application of inks on top of the polycarbonate, the additional requirements listed below shall apply:

   4.1. All the tests mentioned in this chapter shall be concluded on the eID cards and ePassports with the personalized primary portrait, and prove that the areas where colour personalization was applied are not less durable than the polycarbonate-only parts.

   4.2. Contact with the human skin (including fats) shall be considered as a normal usage for the areas protected with the mentioned technology

5. In the durability testing of the proposed ePassport booklets (according to the paragraph 1 of the present chapter), the proposed hinge technology shall be also included, including but not limited to sheet pull sequence, delamination sequence and all thermal and chemical tests.

6. Durability tests mentioned in the current chapter on both ePassport and eID card shall be done with the offered model and electronic configuration of the embedded chip (same model, same type of antenna connection and eID cards with the contact plates) and after the durability test done according to the requirements of this chapter, it must be assured that electronic components still work function properly.

4.3 Electronic passport structure and physical security features

1. The requirements in this section apply to all ePassport booklets given in Table #1.

2. All Passports shall follow in its format the ICAO 9303 Standard.

3. The life span of the passport shall be ten years.

4. The booklet shall be constituted as follows:
   4.1. 48 (forty eight) paper pages (inner pages) and 1 (one) electronic 2-page insertion (Data Page) in polycarbonate material,
   4.2. The data page shall have physical characteristics as specified in the standards for the type of identity documents TD-3, length 125 mm, width of 88 mm and maximum thickness of 0,9 mm for the data page,
5. The booklet is made of the following elements:
   5.1. Cover,
   5.2. End leaves,
   5.3. Inner Pages,
   5.4. Electronic Data Page.

6. Graphical design of end leaves, inner pages and cover shall retain the key design elements of the current Georgian passport but have alterations on end leaves and inner pages which will make it harder for attacker to reuse elements from the current passports (lost, stolen, etc.) to reconstruct high quality forgeries. The graphical design of the current passport booklet is provided through the attachment. As regards to the security features of the graphical design, the supplier is not limited to the current graphical design framework and in particular in relation with the Datapage.

4.3.1 Cover

1. These requirements are valid for all ePassport booklets given in Table #1.

2. The outside cover shall be made of a 10-13 pts thick 100% acrylic coated material saturated with latex; It shall resist to lamination temperature up to 175-185°C. It shall be compatible with high quality lamination of paper used for end leaves.

3. Outside marks (e.g. coat of arms, phrases and booklet label, as defined in the design) shall be printed in hot stamping, using golden ribbons (industrial gold) with clearly defined contours and without any visible defects.

4. Phrases shall be legible and readable; the hot stamping printing provided shall be abrasion-resistant and with perpetual shine.

5. On the cover the supplier shall use colours approved by the purchaser. The approval shall be done in the manner prescribed by this technical document. Cover colour and design files of each booklet will be sent to the winner company after the contract is signed.

4.3.2 End leaves

1. The requirements in this section apply to all passport booklets given in Table #1.

2. End leaves shall be manufactured free of any infrared absorbing or reflecting materials with a weight of 120-140 gr per square meter (+/ - 5 %). The paper shall be composed of white cellulose and least 50% cotton.
3. The core material of the substrates shall not be reactive to UV in other words: “UV dull”.

4. End leaves shall contain:
   4.1. A main motif,
   4.2. Latent image,
   4.3. Text,
   4.4. Micro text produced with intaglio printing which contain two colours or more.

5. Each End leaf shall be compliant with ICAO guidelines and shall include at least, with the following security elements:
   5.1. Fiduciary background (micro-texts, guilloches, numismatic patterns, deliberated errors),
   5.2. IR-split
   5.3. 4 direct tones IR-invisible offset printing,
   5.4. 1 (one) invisible UV offset printing,
   5.5. Microprint,
   5.6. Anti-scanning design.

4.3.3 Inner pages

1. The requirements in this section apply to all passport booklets given in Table #1.

2. Inner pages shall be manufactured free of any infrared absorbing or reflecting materials with a weight of 90gr per square meter (+/ - 5 %).
3. The core material of the substrates shall not be reactive to UV in other words: “UV dull”.

4. The paper shall be composed of wood pulp and at least 50% cotton. Chemical reagents shall be added to the paper to make possible alterations detectable.

5. The paper shall contain:
   5.1. Security fibres invisible to the naked eye and visible under UV light;
   5.2. registered multi-tone watermark and some texts agreed with PSDA (e.g. “Passport” in English and Georgian);
   5.3. Electrotype watermark showing page numbers.

6. Each inner page shall comply with ICAO guidelines and shall count, at least, with the following security elements:
   6.1. Fiduciary background (iris, microtexts, guilloches, numismatic patterns, deliberated errors);
   6.2. IR-split;
   6.3. Rainbow printing with at least two colour transitions (A-B-A);
   6.4. At least 3 direct tones IR-invisible ink offset printing;
   6.5. 1 (one) invisible UV yellow ink;
   6.6. Microprints;
   6.7. Anti-scanning design;
   6.8. UV design for each page;
   6.9. See-through.

4.3.4 Booklet binding

1. The requirements in this section apply to all passport booklets given in Table #1.

2. Passport binding shall be made with security threads and secure sewing technologies.

3. Threads shall be multicolour and made out of 3 (three) individual fibres, each made with a different colour, visible under UV light. Threads used shall rely on a mechanism that assures their destruction under attempts to disassemble the booklet.

4.3.5 Passport numbering

1. The requirements in this section apply to all passport booklets given in Table #1.

2. Passports shall be numbered according to the requirements of the chapter 4.8 paragraph 8. Passport number shall be present on both end leaves. Passport number on the last end leaf shall be additionally printed in 1D barcode. The passport number and the barcode shall be printed in black, with invisible fluorescence under UV in green.

3. Passport number shall be also applied to the booklet using laser perforation in conic from the polycarbonate data page (including) until back cover (including).

4. Number sequences shall be provided to the Supplier after award.

4.4 General requirements for eID cards and ePassport data pages

1. Graphical design of eID cards and ePassport data page shall retain the key design elements of the current (existing before tender announcement) eID card and ePassport but have alterations which will make it harder for attacker to reuse elements from the lost, stolen, etc. eID cards and ePassports belonging to the current model to reconstruct high quality forgeries. The graphical design of the current eID cards (citizen card, permanent and temporary residence cards) is provided through the attachment. As regards to the security features of the graphical design, the supplier is not limited to the current graphical design framework.

2. eMRTD sign shall be displayed on eID card and ePassport data page according to ICAO 9303 standard.

3. Personalized facial image of the document holder on eID card and ePassport data page shall be easy to be authenticated and distinguished from images that can be obtained with personalization technologies available or potentially available to forgers (throughout document's lifetime).

4. Manipulations with the facial image of the document holder on a personalized eID card and ePassport data page by means of personalization equipment, removal or replacement of any layer of the document or its transfer to another document, or its supplementation, for example, with a thin coating, or any other changes in the initial contents should be easily detectable during the first instance check without special equipment.

5. For the purposes of automated authentication of the document holder's facial image, for example, by means of document scanners, the Supplier shall supply an algorithm and software modules for distinguishing the original personalized image from a counterfeit. Algorithm, revealed to PSDA shall, at least, provide basic level of distinction, compared to software modules which may offer more comprehensive checks. Licensing scheme for the algorithm shall allow PSDA to implement the algorithm by its own and distribute it in a compiled form, for authenticating documents issued by PSDA. Software modules delivered to PSDA shall allow free distribution for PSDA-issued document authentication. The algorithm and the software shall assume that verifiers will use generally available sensor technologies to obtain an image that is suitable for analysis. The algorithm and the software modules shall be delivered according to the requirements of the present tender.

6. The document must also include a secondary facial image (ghost image) of the document holder visible from at least the same page as the primary facial image, that contains at least one Level

1 (one) security feature in addition to conventional security printing and surface relief features. Ghost image must be integrated within one of the following structure:

6.1. Transparent or semi-transparent structure

6.2. Under lenticular structure using more than 3 registered images supplementing each other to form high quality portrait of the holder.

7. The structure of eID card and ePassport data page and personalization technology must ensure that several layers of the card and data page are affected (carbonized) at various depth during the personalization process. It is not allowed to use technologies that personalize only the top layer or use surface coating that is applied only after personalization process (exception from this rule is only permitted for the primary facial image, according to the requirements of the chapter 4.9.5.1 of the present document).

8. During the manufacturing process of blanks (eID cards and ePassport) data pages, polycarbonate layers may only be joined together (laminated) only under high temperature and pressure (no additional binding agents must be used). Only equipment and raw materials fit for this purpose should be used in the technological process.

9. The structure of eID card and ePassport data page must ensure document durability and protection of the electronic component throughout the expected lifetime (10 (ten) years from the date of personalization), must be resistant to physical and chemical decomposition, as well as repeated use of integrated security features for producing counterfeit documents.

10. During the manufacturing process of eID card and ePassport data page, structures of a positive, negative and matt relief that correspond to the approved design and some of these cross the facial image area, must be incorporated in the eID card and ePassport data page surface.

11. Document number shall be duplicated on the back side of eID card with relief structure, protecting main photo of the document holder and at least one biographical information (first name or last name) from attacking from the back side. Font size shall allow verification of the number during the first line of inspection.

12. The document structure should be suitable for obtaining a positive relief for laser engraved elements. Tactile laser engraving positioning is considered on both the obverse and reverse side of the eID card and on the observe side for ePassport data page.

13. eID card must have at least 3 (three) and ePassport data page must have at least 4 (four) integrated optically variable elements, where:

13.1. At least 1 (one) is a diffractive optically variable image device (DOVID) that contains Level 1, Level 2 and Level 3 security features and is not positioned on the top layer of the card or data page, but protects the holder's primary face image;

13.2. At least 1 (one) element is personalized with the holder's data;
13.3. At least 1 (one) element is printed with optically variable ink (OVI);
13.4. At least 1 (one) element is located on the ePassport title page (reverse of the data page) protecting at least the main photo of the document holder from attacking from the back side.

14. Background of the blank eID card and ePassport data page (front and back) shall be printed in offset by including at least the following elements:

14.1. Positive and negative multicoloured guilloche or other fine line patterns that would make it as hard as possible to imitate and reproduce the original image;
14.2. Rainbow printing with at least two colour transitions (A-B-A);
14.3. Anti-copying and anti-scanning security features;
14.4. Positive and negative micro-print.

15. Background printing of the blank eID card and ePassport data page (front and back) shall be supplemented with the UV fluorescent print that is invisible in the daylight (and contrasts with the UV neutral medium). At least the following elements shall be included on the document, some of the elements belonging to the single category shall be included on both pages:
15.1. Multicoloured guilloche and/or other fine line patterns that would make it as hard as possible to imitate and reproduce the original image;
15.2. Rainbow printing;
15.3. Diverse reactions when the UV spectral parameters (wave length) are changed;
15.4. Non-variable picture in high resolution using trichromatic UV colours.

16. Background print of the blank eID card and ePassport data page shall also include elements that can be checked using infrared light (“infrared disappearance”) that complies with the ICAO guidelines regarding the use of optically machine-readable elements.

17. Elements in various printing forms for the background print of the blank eID card and ePassport data page shall be distributed so that it is very difficult to decompose the background print (e.g. separation of the object in smaller components) for counterfeit purposes and the possible manipulations are easily detectable.

18. A document number must be incorporated on front side of the blank eID card during its manufacturing process.

19. Personalized document (eID and ePassport), shall include at least one field laser engraved with a specific (modified) font of the PSDA. Design of the font shall be done by the Supplier and agreed with PSDA.

20. Use of other materials (other than polycarbonate) is allowed in the place of embedding (sewing in) of the data page in the passport blank (referred to as the “hinge” in this document) while ensuring a high level of protection against separation and considering the different physical and chemical properties of the materials. Glue or other adhesives shall not be used to connect the hinge and the data page.

21. The data page structure must be resistant to complete or partial physical and chemical delayering so that in case of any manipulations it leaves visible signs of counterfeiting that can be identified in the first-level check.

22. In making the data page, the hinge and the juncture, it has to be taken into account that the hinge that stretches deep into the data page or forms a full-size data page layer and is made of a different material diminish the polycarbonate data page's structural integrity and protection against separation of individual layers of the data page for counterfeiting purposes. In case of offering such solution, the connection of the different layers of the data page shall be still made of melting them together on the same lamination temperature.

23. The hinge and the method of its integration in the data page and laser personalization must ensure protection both against imitation using a similar or equivalent material and against counterfeiting using the original hinge or a hinge taken from another document. Any attempts to imitate or re-use the hinge must be easily identifiable in the first-line check.

24. It must be possible to add e.g. document number to the hinge at the manufacturing stage.

25. This hinge shall contain level 1 or level 2 security printing or embossing.

26. The blank eID card and ePassport data page may have integrated one security feature (Level 4) which is classified as CONFIDENTIAL. For specification and incorporation of this security feature in the blanks, measures of protecting classified information shall be applied.

27. When preparing design deliverables of the blanks to be approved by PSDA, the Supplier shall choose methods which simulate the effect to be achieved in the end-product as close to the original as possible.

28. PSDA can only accept the colour tones to be used for final product presented on original laminated material.

29. Starting production of the end-product is only permitted after all approvals are received from PSDA.

4.5 General requirements for embedded chip and its software

1. The blank (both eID card and ePassport) must have an embedded software (software running on an underlying chip) with contact and contactless interfaces for eID card and contactless interface for ePassport.

2. Chip module together with an antenna shall be integrated in the blank in such a way that no cracks are formed in the top layers of the card and data page throughout the entire lifetime of a document, that it does not affect other integrated security features and is not damaged during the optical personalization process.

3. Contact plate of the chip (for eID card) must be properly protected against corrosion and wear and tear that may occur during the lifetime of a card (10 (ten) years after personalization) as a result of using the card for its intended purposes.

4. The chip on which the embedded software are designed must be certified according to the Common Criteria at EAL 5+ level at least, by using the security profile BSI-CC-PP-0084-2014 or equivalent.

5. Chip must have security features against existing and potential security threats.

6. Chip used for eID card must have a memory (EEPROM or FLASH) that ensures at least 70 kilobyte of free memory space after loading necessary applets, before personalization. Memory space for ePassport chip must be sufficient to personalize intended data set with high quality facial image. Chip used for eID card must be Type A chip according to ISO/IEC 14443. If eID card does not contain Auxiliary Data Application, it shall have MIFARE Classic contactless card emulation possibility (1 (one) kilobyte memory at least).

7. Chip must have symmetrical and asymmetrical cryptography coprocessors which support AES, 3DES, RSA and ECC algorithms.

8. Chip must support 424 Kbps data transmission speed in contactless.

9. **For eID card**, the embedded software must be a javacard operating system (javacard platform). It shall also contain one javacard applets offering the following applications:
   9.1. The application implementing the features required for the “eMRTD application” – this application is mandatory for all cards delivered in the scope of the current purchase;
   9.2. The application implementing the features required for the “IAS Application” – this application is mandatory for all cards delivered in the scope of the current purchase with all features described in sub-chapters of the chapter 4.6, except chapter 4.6.7 (Support of chapter 4.6.7 is mandatory as soon cards are delivered with Auxiliary Data Application).

9.3. The application implementing the features required for the "Auxiliary Data Application" – supply of this application is conditional and the Supplier has right to deliver initial sets cards without it (see chapter 3.2 for details).

10. **For ePassport**, the embedded software may be a javacard operating system (javacard platform) with one javacard applet implementing the features required for the "eMRTD application" (see description below), or a native application implementing the features required for the "eMRTD application" (see description below).

11. The following functionality must be supported:

    11.1. For eMRTD Application - The electronic machine-readable travel document with the facial image and fingerprint biometry protected by BAC, PACE, Chip Authentication, Terminal Authentication and Passive Authentication security mechanisms— during the period of validity of the Contract, the Supplier shall ensure compliance with the most recent technical specifications underlying applicable European Union laws and regulations regarding machine-readable travel documents. This application is used for both documents – eID card and ePassport.

    11.2. For IAS Application - Qualified electronic signature creation device that can be also used for electronic identification and authentication of its holder and for protection of electronic communication— during the period of validity of the Contract, the Supplier shall ensure compliance with the most recent technical specifications underlying applicable European Union laws and regulations regarding electronic identification and qualified electronic signature.

12. Operating system using JavaCard platform (for eID card and optionally ePassport), must be certified according to the Common Criteria at EAL 5+ level at least, by using Java Card Protection Profile – Open Configuration (or equivalent), that allows to install additional apps in the electronic component throughout its lifetime without affecting functionality, security and the relevant certification of its main applications.

13. Operating system of the chip must meet the following standards (equivalence means full compatibility in publicly known functionality):
    13.1. Java Card 3.0.4. CE or newer (or equivalent) – mandatory for eID card, optional for ePassport
    13.2. Global Platform 2.2.1 or newer (or equivalent).
    13.3. Operating system of the electronic component shall support secure channel protocols SCP02 and SCP03.

14. The “Auxiliary Data Application” shall provide storage capability on contact and contactless interface, to store person-specific data on eID card. It shall correspond to the requirements of chapter 4.6 – Detailed functional requirements of IAS and Auxiliary Data Applications.

15. The eMRTD application shall ensure ECC (Brainpool and NIST curves are mandatory) and AES cryptographies, as well as SHA-2 hash function support in all applicable security mechanisms and protocols (except Active Authentication and Basic Access Control).

16. The eMRTD application is expected to personalize at least DG1, DG2, DG3 (DG3 shall be protected with the terminal authentication mechanism), DG7, DG11 and DG12, as well as data groups related to implementation of security mechanisms. Detailed configuration of the file system and security mechanisms shall be agreed between the PSDA and Supplier after conclusion of the Contract. Personalization of DG3 shall be optional for eID card.

17. The eMRTD application shall support dynamic binding, it is not allowed to use static contactless identifier (UID or PUPI) for ePassports.

18. The Supplier shall ensure delivery of personalization keys of the electronic component to PSDA. Personalization keys must be replaceable during the personalization process. Delivery of the personalization keys shall assume transportation using key-exchange-key (KEK) delivered to the 3 (three) separate key custodians at PSDA. Delivery of KEK and other keys shall happen using the procedure outlined in the chapter 4.10:

19. The IAS Application shall ensure RSA and ECC cryptography support for the following core functions:

    19.1. Electronic identification of a cardholder.
    19.2. Electronic authentication of a cardholder.
    19.3. Creation of a qualified electronic signature.
    19.4. Protection of electronic communication (encryption and decryption).

20. X.509 certificates required for performing core functions listed above may be issued by a trust service provider whose services are not a subject of this procurement. The Supplier is responsible for providing all necessary information regarding qualified electronic signature creation device to be supplied by the Supplier that is required during accreditation of the trust service provider or regular audit process.

21. Authentication and qualified electronic signature creation functions must be protected with two separate PINs (PIN_{auth} and PIN_{sig} respectively) which are blocked after 3 unsuccessful PIN attempts.

22. PIN_{auth} shall be shared with eMRTD application and it shall be possible to read DGs after PIN_{auth} authentication.

23. It is permissible to use in the solutions only such cryptographic algorithms (symmetrical and asymmetrical), key lengths, hash functions and other data protection mechanisms which guarantee security throughout the lifetime of the document pursuant to recommendations of competent authorities, such as certification bodies.

24. Cryptographic functionality of the electronic component of an eID card shall be tested and certified according to the Common Criteria EAL 4+ or higher, using protection profiles defined by relevant parts of EN 419211 (at least EN 419211-2:2013, EN 419211-3:2013, EN 419211-4:2013 or their newer versions of the standards or respective profiles).

25. The eID card shall allow future evolution through the lifetime of the card (loading of the new application, new functionalities…). In particular, it shall be possible to fully deactivate IAS Application and loading and personalizing the new IAS Application with the similar functionality.

26. IAS Application shall correspond to the requirements of chapter 4.6 – Detailed functional requirements of IAS and Auxiliary Data Applications.

27. The Supplier shall specify detailed requirements for the electronic component software (electrical profile) in cooperation with the PSDA after conclusion of the Contract. The Supplier shall follow the current profiles of ePassport and eID card as much as it is possible and feasible, and get PSDA's approval prior to implementation.

28. The PSDA shall be given at least 10 (ten) working days for approving any deliverable related to specifying details of the software requirements. Production of the end-product may be started only after approval of a specification of the electronic component and its software by the PSDA.

29. All functions of the embedded chip and its software must be documented at the APDU level. Publication of eID card interface descriptions (specification) falls within the PSDA's competence and Supplier is not entitled to restrict it. The only exception from this rule may be specification of the personalization commands which may be covered with non-disclosure agreement (NDA).

30. It shall be possible to personalize IAS and eMRTD applications in a fully secure mode where all traffic to and from the embedded chip will be encrypted and protected with MAC codes

31. If eID card chip supports MIFARE option, the following requirements shall be satisfied:

31.1. eID card shall also provide API (application programming interface) to applications (applets) stored inside eID card chip allowing them to read and modify data stored in MIFARE

31.2. MIFARE Application Directory structure shall be initialized before the cards are delivered to PSDA

31.3. MIFARE security keys shall be initialized with non-default values ensuring uniqueness of the keys for cards, as well as the sector, with exception of the key A of the sector 0 (MAD key). The security keys or their derivation data shall be delivered to PSDA

4.6 Detailed functional requirements of IAS and Auxiliary Data Applications

4.6.1 User's Cryptographic Keys and Certificates

1. Cryptographic key pairs (PrK_{auth} PuK_{auth}) for authentication and (PrK_{sig} PuK_{sig}) for digital (qualified electronic) signature shall be generated by IAS Application as a response of key generation command issued by the terminal. It shall be possible to generate and re-generate each key pair individually in unlimited number of times – corresponding to number commands issued by the terminal. RSA-2048 and ECC-256 shall be supported as key types. It shall be possible to choose key type at least during card personalization. Secure import of the key pairs shall be also supported
2. Keys PrK_{auth} and PrK_{sig} shall be securely stored inside the chip (ICC hereafter) only, without any possibility to export them outside, including export in encrypted form. It shall be possible to maintain constant references (by using static key identifier, placing key identifier in some file with pre-defined path, or some other means) for each key.
3. It must be possible to perform digital signature operation using PrK_{auth} as well as PrK_{sig} keys. At least PKCS#1 v1.5 scheme shall be supported for RSA keys. If user's PC is equipped with corresponding software, it shall be possible to use (PrK_{auth} PuK_{auth}) key pair for client authentication in SSL/TLS sessions. Also, PrK_{auth} key shall be usable for deciphering data, enciphered using PuK_{auth}.
4. When IAS Application is personalized, operations involving PrK_{auth} or PrK_{sig} shall require user authentication. Cryptographic operations (digital signature, online authentication, decipherment, etc.) shall require authentication with PIN_{auth} and PIN_{sig} respectively.
5. IAS Application shall be able to store at least two X509 certificates whereas one corresponds to PuK_{sig} another correspond to PuK_{auth} in its file system. It shall be possible to distinguish each of them from other objects stored in IAS Application file system
6. IAS Application shall be able to store at least two X509 certificates (certification authority certificates) in its file system. It shall be possible to distinguish each of them from other objects stored in IAS Application file system
7. IAS Application shall be able to store at least 2 more optional certificates. At least 2 types, X509v3 PKI certificates and X509 attribute certificates shall be supported. If the corresponding space is unused, it shall be detectable (for example, by using some metadata stored in IAS Application like file size equals to zero, file does not exist, etc.)

8. In post-personalization phase it shall be possible to replace certificates with new ones, in unlimited number of times. For optional certificates described in paragraph 7 of the present chapter, it shall additionally mean possibility of deployment in previously unused space and also marking used space as unused (certificate removal)
9. All certificates shall be freely readable from contact interface of ICC without requiring secure session and/or user authentication
10. All operations after IAS Application personalization which involve contactless interface of ICC including certificate reading shall require secure session
11. Once IAS Application is personalized, operations such as certificate management (deployment and/or removal) and generation of (PrK_{auth} PuK_{auth}) and/or (PrK_{sig} PuK_{sig}) key pairs shall require user's authentication with PIN_{auth} and authentication of a terminal as User Key and Certificate Management Terminal.
12. Certificate signing request (CSR) for PuK_{auth} and PuK_{sig} shall be integrity-protected, when they are exported from the IAS Application. Integrity-protection method shall be chosen in a way which guarantees authentication of the CSR in certification authorities responsible to issue user certificates and proving that keys were indeed generated by IAS Application. One of following mechanisms shall be used:
    12.1. Chip authentication key pair (according to chapter 4.6.6 - Extended security mechanisms) shall be used to digitally sign certificate signing requests before exporting them from IAS Application. CSR shall also contain unique identifier of eID card (for example, document number according to the paragraph 14)
    12.2. Certificate requests shall be only performed in secure messaging mode, established using chip authentication (according to chapter 4.6.6 - Extended security mechanisms), with Source-MAC, Response-MAC and Encryption mechanisms enabled.
13. IAS Application file system shall have possibility have separate elementary file, to store at least 64 bytes of binary data there. File content will be written during personalization and once IAS Application is personalized, file shall become readable only if user is authenticated with PIN_{auth} and be accessible from contact interface at least.
14. IAS Application file system shall have possibility to store document number in a separate elementary file. The document number shall be written either before delivering eID cards to PSDA (in this case, PSDA shall not have right to change it), or PSDA shall have right to write document number during personalization and protect from the unauthorized change. Document number shall be readable from contact and contactless interface (reading it from the contactless interface shall require PACE session to be established in accordance with the chapter 4.6.4). Document number shall be readable in the secure messaging mode established using chip authentication.

4.6.2 User authentication and password management

1. User authentication for operation shall mean providing user password to IAS Application. All passwords shall be static and numeric.
2. At least 3 passwords, PIN_{auth}, PIN_{sig} and PUK shall be supported.

3. Additional password, $PIN_{transport}$ may be additionally supported or, alternatively PUK can be used instead of $PIN_{transport}$. If PUK is used in the role of $PIN_{transport}$, all requirements to $PIN_{transport}$ shall apply to PUK (in addition to the requirements for PUK itself) and shall not be understood as mandatory requirements for supporting $PIN_{transport}$.as a separate password.
4. PIN_{auth} shall be at least 6 (six) digits long and be a blocking password.
5. PIN_{sig} shall be at least 6 (six) digits long and be a blocking password.
6. PUK shall be at least 8 (eight) digits long. It shall be a blocking password and have limited usage number. Usage number shall be either fixed to 10 (ten) or defined during personalization and the purchaser shall be able to have limit set to value 10 (ten). Once usage number of PUK reaches zero, it shall draw PUK unusable - any attempt of use shall end with error code "Blocked". It shall be possible to read PUK usage number using APDU commands
7. $PIN_{transport}$ shall be at least 5 (five) digits long and be blocking password. It shall share its PRC with either PIN_{auth} or PUK.
8. All blocking passwords shall have password retry counter (PRC) set to initial value of 3 (three) either during personalization or pre-defined.
9. Once invalid value of the blocking password is provided, PRC shall be decreased by 1 (one).
10. Once valid value of the blocking password is provided and PRC does not equal to 0 (or value equal to 1 (one) in case if contactless interface is involved), value of the PRC shall be restored to initial value of 3 (three)
11. In case if PRC equals to 1 (one), IAS Application shall not accept any further authentication attempts from contactless interface (at least in PACE mode) and respond with error code "Suspended". In this case, IAS Application shall still accept authentication attempt from contact interface.
12. In case if PRC equals to 0 (zero), IAS Application shall not accept any further authentication attempts from either contact or contactless interface and respond with error code "Blocked"
13. PUK can be used to reset PRC back to initial value (3) for PIN_{auth} and PIN_{sig} and it shall cause decrease of PUK usage counter by 1 (one)
14. During personalization, at least PUK and $PIN_{transport}$ shall be set.
15. PIN_{sig} shall not be set during personalization.
16. IAS Application may permit not to set PIN_{auth} during personalization.
17. If some password (PIN_{sig} at least and maybe PIN_{auth} also) is not set, IAS Application functionality protected with respective password shall be unavailable before setting proper value to the password. Legitimate cardholder shall be able to use $PIN_{transport}$ to set value. Once value of the password is set, $PIN_{transport}$ shall not be usable to set value once again (Note: in case if PUK is used as $PIN_{transport}$, it may be still possible based on other requirements of this chapter designated for PUK).
18. If the terminal is authenticated as "Password Management Terminal", it shall be possible to switch personalized IAS Application instance in the following state:
    - 18.1. All PRCs, as well as PUK usage number shall be reset to their original values;
    - 18.2. PUK and $PIN_{transport}$ set to new values
    - 18.3. PIN_{sig} cleared, which also results invalidation of (PrK_{sig} PuK_{sig}) key pair and deletion of corresponding certificate in atomic operation
    - 18.4. PIN_{auth} either cleared, or set to new value

19. Authentication with either PIN_{auth} or PUK shall be required to set new value of PIN_{auth}. In case if PUK is involved, this operation shall also reset retry counter of PIN_{auth} to initial value (3) and decrease PUK usage number by 1 (one).
20. Authentication with PIN_{sig} shall be required to set new value of PIN_{sig}. IAS Application may additionally permit usage of PUK for setting a new value in case if and only if the terminal is authenticated as "Password Management Terminal". In case if PUK is involved, this operation shall also reset retry counter of PIN_{sig} to initial value (3) and decrease PUK usage number by 1 (one).
21. Authenticated state of PIN_{sig}, $PIN_{transport}$ and PUK shall be invalidated right after executing subsequent operation which requires authentication with respective password. Invalidation means the similar command given to ICC again shall again require authentication. For example, authentication state of PIN_{sig} shall be invalidated by digital signature operation which involves PrK_{sig} , but it shall not be invalidated by certificate reading command (since certificate reading does not require PIN authentication). Even if the complex command is issued (e.g. CHANGE REFERENCE DATA APDU with old and new values of PIN_{sig} meaning authentication and PIN change at once), it shall be treated internally like second command was also issued, and invalidate authenticated state of respective password. The state shall be invalidated also after deselecting IAS Application or resetting ICC.
22. Authenticated state of PIN_{auth} may be invalidated after changing its value. Authenticated state shall be invalidated after deselecting IAS Application or resetting ICC.
23. Principles of authentication invalidation and password blocking shall be followed regardless the fact how the commands are formatted: sent in compound form ICC (e.g. CHANGE REFERENCE DATA APDU which accepts both and new password and implicitly means authentication first and then password change), or sent in separated form(e.g. authentication command is sent first and then it is followed with CHANGE REFERENCE DATA APDU with new password only).

4.6.3 Applet Selection and Identification

1. Functionality provided by IAS Application, if it is not related to Master File functions (e.g. PACE), shall be accessible via one or more Application Dedicated Files (ADFs) selectable according to ISO/IEC 7816.
2. IAS Application instance shall be identified using Application Identifiers (AID) equal to D250 00001601 (RID=D250000016, PIX=01)
3. During selection of at least one ADF of IAS Application, FCP parameters shall be returned in such a way that it shall be possible to get the following information: Application version (major, minor) and applet lifecycle status (non-personalized, personalized, etc.). Major version shall be 3(three).
4. If Auxiliary Data Application assumes separate Application Dedicated File (ADF), the following requirements shall apply:
   4.1. Auxiliary Data Application instance shall be identified using Application Identifiers (AID) equal to D250 00001601 (RID=D250000016, PIX=02)

4.2. During selection of at least one ADF of Auxiliary Data Application, FCP parameters shall be returned in such a way that it shall be possible to get the following information: Application version (major, minor) and applet lifecycle status (non-personalized, personalized, etc.).

4.6.4 Secure Sessions and auxiliary keys

1. IAS Application shall be able to maintain secure session and require such sessions for security-critical operations
2. All secure sessions shall be established in encrypt-then-authenticate form. At least, request from the terminal to the applet shall be protected by this method.
3. After personalization of IAS Application, access to it using contactless interface shall require establishment of secure session using password-based authentication (PACE protocol) before all operations
4. PACE protocol shall be implemented in accordance with ICAO requirements for Machine Readable Travel Documents (ICAO Doc 9303).
5. PACE functionality shall support PIN_{auth}, as well as CAN- and MRZ-password, but authentication with MRZ and CAN shall be reserved to other card applets like eMRTD Application. Sessions authenticated with CAN or MRZ shall be treated like unauthenticated ones in IAS Application functionality.
6. Once authenticated with PACE and respective password, it may be possible to perform operation which requires user authentication based on corresponding password. This option shall be available for PIN_{auth}
7. Contact interface shall allow both secure (with PACE) and insecure access
8. PACE authentication shall be available as a global card service. That is, it shall be usable for other applets deployed on ICC (eMRTD and Auxiliary Data Applications). In particular, same PACE capability shall be usable for eMRTD Application to enable Supplemental Access Control. This shall be a case for PIN_{auth} and MRZ and not be a case for PUK, PIN_{sig} or $PIN_{transport}$. Moreover, possible compromise of this "global service" (for example, by compromising post-personalization key set which may allow deployment of bogus applets on the card or even replace the legitimate ones) shall not bear risk of performing cryptographic operations with (PrK_{sig} PuK_{sig}) key pair by adversary.
9. Once secure session is established, all other password authentications shall be possible using VERIFY APDU command and plaintext password
10. Contact interface shall allow both PACE-authenticated secure session and plain, unauthenticated sessions. In the latter case, all password authentications shall be possible using VERIFY APDU command and plaintext password
11. All ephemeral keys shall have maximum security supported by the ICC platform

4.6.5 Compatibility with Smart Card Readers

1. All functionality which is designated for the final customer's PC to work with the smart card (with or without the middleware, defined by the present tender) in insecure (not involving secure messaging) mode, must be available with standard length APDU commands and

responses. It's permitted to use extended length APDU commands and responses in parallel. For personalization commands and security-related commands such limitation does not exist
2. Plaintext offline PIN commands (verification and management) shall be supported on contact interface for PIN_{auth}, PIN_{sig}, $PIN_{transport}$ and PUK.

4.6.6 Extended Security Mechanisms

1. IAS Application shall support chip authentication and terminal authentication. These protocols and their versions shall correspond to protocols and versions, permitted by ICAO Doc 9303.
2. At least, 256-bit Elliptic Curve (EC) keys and BrainpoolP256r1 curve shall be supported
3. IAS Application shall have possibility to prove the chip is genuine, without involvement of eMRTD Application (usage of DG14 file and digital signature using Document Signer) – for example, by relying on passive authentication of the chip authentication key based on the special Certification Authority.
4. Chip authentication public key shall not be readable from ICC without user authentication (according to chapter 4.6.2 – User authentication and password management) - via contactless interface at least
5. At least the following types of the privileged terminals shall be supported via terminal authentication:
   5.1. Certificate Management Terminal
   5.2. Password Management Terminal
6. IAS Application shall have possibility to hold data for 2 (two) CVCA which is sufficient to perform Terminal Authentication. At least one CVCA data will be deployed during personalization. The following requirements shall additionally apply:
   6.1. It shall be possible to issue certificates for the privileged terminals with certification authority different from DVCAs (certification authorities, certified by the same CVCA for issuing inspection system certificates for accessing eMRTD application) and making sure DVCA-issued certificates will not be treated as privileged terminals;
   6.2. It shall be possible for the privileged terminals to use CVCA link certificates for updating CVCA references, and this capability shall not deny inspection systems (the systems operating with DVCA-issued certificates) to also use CVCA link certificates for the similar purposes;
   6.3. If IAS Application and eMRTD application share the same CVCA data, it does not mean CVCA link certificates supplied to inspection systems and privileged terminals shall contain same data in each and every fields and extensions (obviously, fields like certification authority reference, public key, certificate holder reference, expiration date will be same).
7. To authenticate terminal as a privileged terminal, like Certificate Management Terminal or Password Management Terminal, chip authentication shall be performed first, followed by switch to secure messaging mode with ENC, S_MAC and R_MAC mechanisms enabled, and terminal authentication with respective rights
8. IAS Application shall be able function in normal, "unprivileged" mode after successful chip authentication and switching to corresponding secure session, if there was no terminal authentication attempt (e.g. cryptographic operations using (PrK_{auth}, PuK_{auth}) or (PrK_{sig}, PuK_{sig})

key pairs shall be possible in this mode – with necessary prerequisites specified in the present document)

9. Once authenticated with respective terminal certificate, Certificate Management Terminal and Password Management Terminal shall not have right to perform cryptographic operations using (PrK_{sig}, PuK_{sig}) key pair
10. If the terminal authenticates itself as a privileged terminal, bringing ICC back to "normal" (unprivileged) mode after completing this work shall not require to reset ICC (neither with warm reset, nor cold reset)

4.6.7 Requirements for Single Sign On Capability

1. IAS Application shall provide the Single Sign On capability to 3rd party applications which may be later deployed on the eID card chip by PSDA. In particular, it shall let other applications in other JavaCard packages to use functionality of IAS Application for their needs, via javacard.framework.Shareable or the similar mechanism which allows inter-applet communication through the applet firewall.
2. The capabilities which shall be shared are listed below:
   2.1. PACE using PIN_{auth} and CAN (supporting other passwords is optional);
   2.2. Plaintext PIN_{auth} verification;
   2.3. Chip authentication, including ensuring authenticity of chip authentication keys;
   2.4. Terminal authentication;
   2.5. Reading the document number written in IAS application;
3. Sharing of the PACE mechanisms may be limited as follows:
   3.1. It is not mandatory to let other applets to use PACE channel established with MF (master file) and it is acceptable to require establishment of the secure channel with the file different from the MF (e.g. Application-specific ADF). However, PACE domain parameters and other publicly readable PACE-related data should be still left written in MF;
   3.2. Decrease of PIN_{auth} retry counter if the validation fails, and blocking PIN_{auth} if the counter reaches zero.
4. Sharing of the plaintext PIN_{auth} verification capability may be limited to checking PIN value (with decrease of PIN_{auth} retry counter if the validation fails, and blocking PIN_{auth} if the counter reaches zero).
5. Sharing of the chip authentication mechanism may assume that APDU commands will be sent from the terminal to the file other from MF (e.g. Application-specific ADF), and the secure channel will be established with it.
6. Sharing of the terminal authentication may be limited to validation of the terminal certificates against CVCA, with update of CVCA references if the link certificate was presented.
7. When implementing this capability, IAS Application shall never return PIN_{auth} in plaintext to other applications.
8. It is permitted for IAS Application to assume all APDU commands with the terminal will be handled by the 3rd party application. However, APDU command based exchange with the 3rd

party application is also possible, provided that the 3rd party application will have possibility to monitor statuses of response APDUs returned from the IAS application.

9. The Supplier shall deliver sample application in compiled and source code form, showing example of using all these shared capabilities. Delivery shall happen no later than eID cards with the single sign on capability.

4.6.8 Requirements for Auxiliary Data Application

1. Auxiliary Data Application shall allow PSDA to store additional information about the card holder on eID card with his/her consent. Example of the information is student status, loyalty card information, etc. The Auxiliary Data Application shall support user authentication with PIN_{auth} which shall be same as, and managed by IAS application. Authentication with PIN_{auth} on the contactless interface shall require PACE protocol.
2. The Auxiliary Data Application shall be accessible through contact and contactless interface. If not explicitly mentioned, all requirements of the present chapter apply to both interfaces.
3. The Auxiliary Data Application shall be capable of storing arbitrary data in Elementary Files (EFs).
4. All content-related operations on EFs shall be possible using APDU commands according to ISO/IEC 7816 part 4. In particular:
   4.1. File selection - SELECT APDU
   4.2. File content management - UPDATE BINARY (optionally - WRITE BINARY, ERASE BINARY)
   4.3. Reading content of the file - READ BINARY
5. Auxiliary Data Application shall support at least 32 (thirty two) EFs simultaneously. If it is not possible for PSDA to dynamically create more EFs as needed, it shall be possible for PSDA to request the Supplier to extend this number for the next deliverables of the eID cards in the scope of the current purchase – considering the limitations of the chip modules used in eID cards.
6. PSDA shall have right to assign identifier containing at least 2 (two) bytes to EF, or remove the assignment. Auxiliary Data Application shall support selection of the EF using this identifier with SELECT APDU command according to ISO/IEC 7816 part 4. PSDA shall be a sole party to decide what identifier values it will use during the assignment. At the Supplier's discretion, file identifier assignment may mean creation of the file, and un-assignment may mean deletion of the file.
7. without limitation on the number of operations, PSDA shall have right to make individual EF either:
   7.1. Publicly readable – no action from the user (e.g. establishing PACE channel, authentication with PIN_{auth}) is required, the terminal can always read it;
   7.2. Readable through authenticated sessions (when user is authenticated with PIN_{auth})
   7.3. Readable through PACE (at least when PACE is established using CAN or PIN_{auth})
   7.4. Support of other access conditions is optional.
8. If the EF is not set as publicly readable, its reading for contactless interface shall be possible only if PACE channel is established.

9. If the EF is set as "publicly readable", the Auxiliary Data Application may still rely on cryptographic operations (like symmetric keys with or without key diversification support) but no restriction like purchase of the special hardware, payment of royalty fees, etc. shall be imposed to neither PSDA nor third parties who want to read such files.
10. Chip authentication protocol shall be supported by the Auxiliary Data Application. If the EF is not set as "publicly readable", it shall be possible to read the data from it in the secure channel established with chip authentication protocol, provided that the access conditions as required in paragraph 5 are also met. Authentication of card's chip authentication keys shall be possible.
11. Support of different access conditions for EFs for accessing them from contact and contactless interface are not required.
12. File content management operations (paragraph 4.2), as well file identifier assignment and un-assignment operations (paragraph 6) and security attribute assignment operations (paragraph 7) , shall be possible if and only if the card holder is authenticated and the privileged terminal is acting: In particular:
    12.1. The user shall be authenticated with PIN_{auth};
    12.2. Chip authentication session shall be established;
    12.3. The terminal shall be authenticated according to chapter 4.6.6 (Extended Security Mechanisms). For terminal authentication, is not allowed to require Password Management Terminal rights, however it is possible to use Certificate Management Terminal rights or to introduce a new type of privileged terminal.
    12.4. No other security mechanisms shall be mandatory.
13. It is possible to make Auxiliary Data Application separate from IAS application and use single sign on capability (chapter 4.6.7) of the IAS application when PIN_{auth}, CAN, chip authentication or terminal authentication is required.

4.7 Requirements for the middleware

1. The middleware must ensure that "IAS Application" features of the eID card become available to relying applications on target operating systems and computing devices, using standard interfaces. The middleware must be developed by using open standards and documentation, supplementing the current middleware used by the PSDA, and by retaining full support for the currently issued eID cards.

2. After conclusion of the Contract, the PSDA will provide the Supplier with an access to the existing source code which is based on OpenSC library, and documentation of the middleware. Source code access will be granted on PSDA's git repository. Versions shall be assigned to Middleware deliverables provided by the Supplier, and the same version strings need to be identifiable in git repository (e.g. by naming tags accordingly).

3. The Supplier is required to ensure subsequent management of the middleware source code on a platform approved by PSDA and by granting the PSDA free access to the source code and ensuring a possibility to determine its publication policy.

4. Terms and conditions for the middleware licence shall be defined by the PSDA, and the Supplier is not entitled to retain intellectual property rights related to the middleware.

5. The Supplier is responsible for ensuring timely support of the middleware for the most recent versions of Microsoft Windows 7, 8.1, 10 and above, Apple (macOS) 10.9 and above and Linux (Ubuntu linux 12.04 and above, may be limited to LTS only) operating systems during the period of validity of the Contract, by means of smart card and cryptographic object processing methods, such as CNG, MS CAPI (MS CAPI may be supported through CNG), Minidriver, CryptoTokenKit that are specific to each operating system. PKCS#11 shall be supported for all platforms.

6. The middleware shall ensure at least the following minimal functionality:

    6.1. Electronic identification of a cardholder — data acquisition (reading) from the data group and/or certificate of the "IAS Application" of the electronic component of an eID card, including reading of the relevant certificates, with a possibility to perform unilateral or bilateral authentication.

    6.2. Electronic authentication of a cardholder by means of authentication certificate and relevant authentication private key, where the cardholder is required to enter the secret PIN_{auth}.

    6.3. Creation of a qualified electronic signature by using the data to be signed or related hash value, cardholder's qualified certificate and relevant private key of the electronic signature (data for creating an electronic signature), where the cardholder is required to enter PIN_{sig}.

    6.4. Decryption of a value encrypted by a public key by using the encrypted value and relevant private key, where the cardholder is required to enter the secret PIN_{auth}.

4.8 General requirements for blank document manufacturing and delivery

1. When ensuring the production process of the blanks, the Supplier shall comply with the requirements of ISO 14298:2013 or an equivalent standard. Production facility where blanks will be produced shall be certified according to the requirements of ISO 14298:2013 or an equivalent standard, guaranteeing that the certificate will be valid throughout the period of validity of the Contract.

2. The Supplier shall ensure complete accountability and traceability regarding security materials used in the production process of the blank documents including defective blanks spoiled in

the production process by keeping a respective accounting system and carrying out full reconciliation in each stage of the production process. The level of detailing auditing records shall be sufficient to account each unit of the security material used in the production process of the blanks. The auditing records shall be inspected by independent auditors on a regular basis by entrusting the audit procedure to persons who are not directly involved in the production and stock accounting processes. It is necessary to draw up and store documents regarding the surplus of security materials and disposal of the blanks which are defective and spoiled in the production process that shall be approved by a high rank official entrusted with the supervision function.

3. Authorized PSDA's officials will be entitled to check compliance of the Supplier's production facility with provisions included in the Technical Specification and observation of relevant procedures in the practice (for example, storage, accounting and use of materials) by informing the Supplier thereof at least one working day before the planned visit to the production facility. The Supplier's representative shall draw up a written report on the visit to the production facility and inspections carried out which shall be signed by representatives of the PSDA and Supplier. If the Supplier's representative refuses signing the report without a reasonable reason, it shall be deemed as concerted. The report may serve as a basis for claims regarding violations of fulfilling the respective obligations (if such are established).

4. Materials which will be used for production of the blanks shall originate from a limited assortment designed for the particular security product and shall be purchased only from trustworthy and certified suppliers of the security materials. The Bidder shall list in its tender bid all suppliers from which materials and/or components required for production of the blanks will be purchased. The change of suppliers may only be possible upon agreement with the PSDA which shall not reject such changes with no valid reason.

5. The Supplier takes responsibility, to ensure complete quality control in the production process regarding the quality of raw materials, intermediate products and the end product, during whole time of the contract validity.

6. Quality check of the produced and/or purchased blank shall be based on its specification, blank specimen and a catalogue of quality tolerance of blanks approved by the PSDA. The Supplier shall include in its tender bid a short description of the company's practice regarding development of the tolerance catalogues with examples for permissible and impermissible variations of quality. The PSDA shall be entitled not to accept tolerances relating to defects of the blank in the place of integrating a facial image, in the machine readable zone (if it can cause problems of optical reading of the document), in the biometric data fields, as well as in the security features (if that may cause suspicion about counterfeits of the document).

7. The blanks shall be delivered to the PSDA site in 67a Akaki Tsereteli Avenue, Tbilisi, Georgia in compliance with Incoterms 2010 DDP (Delivered Duty Paid). Equipment designated for the personalization sites shall be delivered to PSDA to the addresses defined by the present tender requirements in Tbilisi, Kutaisi and Batumi in compliance with Incoterms 2010 DDP (Delivered Duty Paid).

8. The delivered blanks (ePassport and eID card) shall be numbered in the factory in compliance with the requirements of the Technical Specification. Numbering scheme shall satisfy the following requirements:
   8.1. Each document shall have unique number. Also, it is not allowed to assign the same values to two documents of the different type
   8.2. Values shall be alphanumeric, first two characters shall be digits representing last two digits of the printing year
   8.3. The document number shall not contain three digit "6" in sequence (so, numbers containing "666" shall be excluded from the document numbering).

9. The blanks shall be packed in the Supplier's production facility ensuring that:
   9.1. It is easy to detect attempts of unauthorized opening of the package;
   9.2. The maximum weight of each package does not exceed 15 kg.;
   9.3. Only in case of the request from PSDA, the outer packaging bears the indication of the package contents;
   9.4. The blanks are packaged in the wooden boxes in a way which excludes their damage during the storage or transportation.

10. Consignment shall be supplemented with accompanying documents according to the requirements stipulated by PSDA (an invoice with respective details, a list of blanks, their types and document numbers (range of numbers) included in the consignment, as well as an electronic file with the numbers of blanks and identifiers of microchips incorporated in the respective blanks). The above mentioned accompanying documents shall be electronically sent to the PSDA at least 3 (three) working days before the expected time of receipt of the consignment. The document format shall be specified after conclusion of the Contract.

11. Requirements regarding high value freight forwarding shall be complied with in transportation of the blanks including:
    11.1. Manned security of the consignment is ensured;
    11.2. The selected freight forwarder has a flawless reputation and experience in high value freight forwarding;
    11.3. Precise location of the consignment is traceable and accessible by the Supplier and PSDA at any time.

12. After receiving documents at PSDA, the following checks are made:

12.1. Checking whether packaging has not been subject to unauthorized opening during transportation;

12.2. Checking the number of received blanks according to the rules defined by PSDA;

12.3. If any damages to packaging and/or any other incompliance is established, a relevant statement shall be drawn up and the Supplier will be informed immediately thereof.

13. The Supplier shall, upon the PSDA's request, without undue delay share to the PSDA all necessary information required for personalization of the blanks (including, but not limited to, description of the protocol for communicating with the personalization machines, any specific requirements for production process, and any other information which PSDA will need to know in order to set up and execute personalization process).

14. If object of purchase (any document from the table #1) contains some safety features to be incorporated during personalization (e.g. personalizing the transparent structures, tactile engraving of the holder's personal data and so on), the Supplier shall also configure the personalization equipment in order to ensure proper use of such offered safety features, and provide any necessary information to PSDA may need to have for configuring the personalization system.

15. The Supplier shall ensure security certification of the electronic components (chip, operating system and applications) proposed for eID card and ePassport according to the requirements stipulated in the present document, as well as re-certification as needed, during the whole contract period. If some of the component loses its certification status, the Supplier shall without undue delay inform PSDA about this event and take all necessary actions to resume supply of the certified components.

16. For defective blanks discovered by the PSDA (defects due to the Supplier's fault), a statement shall be drawn up once in 6 (six) months at least which is to be signed by authorized representatives of the PSDA and Supplier.

17. The defective blanks are administered by the PSDA.

18. The defective blanks are not returned to the Supplier, except for defect investigation purposes. Return of the defective blanks shall be possible only in case of PSDA's approval.

19. The Supplier shall deliver an additional number of blanks equal to the number of defective blanks together with the next scheduled blank delivery or shall compensate the value equal to the price of such blanks by deducting the respective amount from the next invoice issued to the PSDA.

20. Depending on the actual demand for identity documents (passports, ID cards, etc.), PSDA must be entitled to make changes to the schedule of blank document deliveries at least 6 (six) months before the planned or requested delivery date.

4.9 Personalization of documents

4.9.1 General Principles

1. The personalization management software will be in-house developed by PSDA. One single personalization system will manage the personalization of both cards and passports. All administration functions (Stock, Job order…) will be common for both documents. Servers, as well as Hardware Security Modules (HSMs) for cryptographic operations will be provided by PSDA.
2. The supplier shall provide hardware (with necessary documentation describing the hardware, as well as their configuration guides in English or in Georgian) required for:
   2.1. Personalization of ePassports
   2.2. Personalization of eID cards
   2.3. Development and testing of extensions of personalization machines – at least the following:
      2.3.1. Chip coding (contact and contactless)
      2.3.2. Emulation of the laser engraving (producing image files instead)
   2.4. Mail finishers for PIN/PUK envelopes (chapter 4.9.7)
   2.5. Inserting machines for envelopes (chapter 4.9.8)
3. The Supplier is responsible to fully configure internal parameters and software of the personalization machines to support personalization of the object of purchase (blank documents, given in Table #1) so that it requires minimal or no effort from PSDA personnel.
4. The purchaser plans to implement quality control both inside and outside machines. To implement quality control outside the machine, the quality control software library shall be delivered.
5. All equipment delivered to fulfil requirements of the paragraph 2 shall rely in the ownership of the Supplier and given to PSDA in possession, with obligation of PSDA to follow the equipment operation rules defined by the Supplier. No later than 6 (six) months after expiration of the contract, the Supplier is responsible to safely remove all sensitive information written in the personalization machines under PSDA supervision, and discard the equipment from PSDA's facilities.
6. In order to let PSDA to continue development of the personalization by its own, the Supplier is responsible to organize trainings for PSDA employees. No more than 50 (fifty) people selected by PSDA shall receive at least 40 (fourty) hours of trainings covering the following subjects (detailed agenda and distribution in classes shall be agreed between the Supplier and PSDA):
   6.1. Machine architecture

6.2. Daily care of machines and problem diagnostics
6.3. Introduction of the new document types, including:
6.3.1. Enhancement of laser layout, definition of the new layouts
6.3.2. Contact and contactless coding
6.3.3. Machine vision
6.3.4. Quality control inside of the machine

7. No later than completion of trainings, the Supplier shall provide PSDA all training materials, at least in electronic form, in English or Georgian language
8. The Supplier shall not deny PSDA to use the hardware delivered according to the present chapter for personalizing documents different from ones listed in table #1 at PSDA's sole discretion, provided that the size and form factor of the documents will match to the machines' specification, the substrates where the laser engraving is assumed will meet recommendations of the manufacturer of the respective machines. The Supplier shall not require any additional expenses and costs from PSDA, except cost of inks for colour personalization (if applicable).

4.9.2 Personalization sites and their performance

1. Personalization shall be performed on three separate sites for all documents (eID cards and ePassports) given in table #1:
1.1. Tbilisi – 2, Sanapiro street, Tbilisi, Georgia
1.2. Kutaisi – 20, Irakli Abashidze street, Kutaisi, Georgia
1.3. Batumi – 7, Sherif Khimshiashvili street, Batumi, Georgia

2. Personalization site maps are provided for information in the attachments. The Supplier shall consider areas and layout of the working rooms of the personalization centers and before supplying the hardware, agree their placement to PSDA. PSDA has right to refuse the proposed placement if it does not ensure normal working conditions for PSDA's staff.

3. Personalization equipment shall be adapted to these environmental conditions:
3.1. Electricity – Single phase, 220V or 3-phase (380V, N, PE), 50hz
3.2. If any other input (like compressed air) is required, the equipment for generating such an input (e.g. air compressors) shall be also provided without any additional expenses and costs.

4. The machines setup on each site shall support the following instantaneous throughput (without using the backup capacity) measured in units per hour (UPH), and considering the primary image resolution on the personalized document will be at least 600 dpi and for other optical data it will be at least 360 dpi:

Personalization Site	Cards		Passports	
	Normal	Peak	Normal	Peak

	Production (one shift, 7.5 h)	Production (two shifts, 15 h)	Production (one shift, 7.5 h)	Production (two shifts, 15 h)
Tbilisi	180 UPH	230 UPH	160 UPH	240 UPH
Kutaisi	65 UPH	70 UPH	55 UPH	60 UPH
Batumi	65 UPH	70 UPH	55 UPH	60 UPH

5. To ensure quick replacement of the personalization machines in emergency cases, the Supplier shall provide at least one printing machine for passports and one for ID cards (or one combined machine), in each personalization site. The following requirements shall additionally apply:
   5.1. The capacity of backup machines shall be enough to ensure operation of the respective personalization site with the capacity demand matching to the normal production (paragraph 4) if the single personalization machine fails;
   5.2. The Supplier shall acknowledge that PSDA will use the backup machines in daily operation with low load (e.g. to print the documents which need to be issued the same day) to ensure the machine is kept at working conditions all the time.
6. Mail finishers for PIN/PUK envelopes, as well as inserting machines shall be supplied in a way which will match peak production capacity for ID cards (see paragraph 4). It is not mandatory to deliver the backup capacity.

4.9.3 Personalization equipment requirements

1. The laser personalization machines shall provide a resolution 700dpi or more;
2. Card Personalization shall be done in 1 (one) pass (including, but not limited to, laser engraving, chip coding, quality control), assuming:
   2.1.1. On board key generation;
   2.1.2. Certificates preparation at PrimeKey EJBCA operated by PSDA.
3. Passport personalization shall be done in 1 (one) pass (including, but not limited to, laser engraving, chip coding, quality control);
4. For full ICAO compliance, the optical personalization device shall support an integrated camera system for positioning of data field against document borders (for MRZ lines) and printed artwork.
5. The eID card personalization machine shall integrate an input tray of at least 200 (two hundred) cards.
6. The personalization device shall support an integrated camera system and extensible quality control software for the verification of the data engraved on the document.
7. Internal software of personalization machine shall be configured by the Supplier for personalization of the offered object of purchase (blank documents, given in Table #1). It must provide the network interface enabling the purchaser's software to perform the following actions:

7.1. Send from the remote system one or more job in structured format (e.g. XML, JSON or ASN.1) to the machine to personalize the blank document(s). Sample data for personalizing each document type from the table #1 shall be provided to PSDA.

7.2. After completion of every stage of document personalization, receive the document status together with the document number printed on the document in the remote system in structured format. Sample remote system shall be delivered in the VmWare virtual appliance form. Related source code written in Java or C# programming language shall be also delivered, letting the Purchaser to re-use and modify it without any limitation;

8. Document personalization capabilities inside the personalization machine shall be configured for each document type from the table #1. It shall include:

8.1. Personalization of electronic carrier:

8.1.1. Personalization using APDU command exchange with the electronic carrier, also exchange of data in structured format (e.g. JSON, XML or ASN.1) with the remote system. For demonstration purposes it is allowed to just demonstrate issuance of self-signed X.509 certificates by the remote system on user's keys generated on eID card.

8.1.2. Sample remote system covering needs of 8.1.1 shall be delivered in the VmWare virtual appliance form. Related source code written in Java or C# programming language shall be also delivered, letting the Purchaser to re-use and modify it without any limitation;

8.1.3. Sample security keys, different from the ones used for the object of purchase (documents from the table #1 including specimen documents) shall be used to for communication with the embedded chip.

8.2. Quality control software inside the machine shall be trained for optical character recognition of biographic data (including English and Georgian characters) and MRZ and shall be configured to verify the laser engraved data against the job data during personalization of the documents from the table #1. The configuration shall be separated to laser engraving template, so that change in laser template shall also require change in the quality control configuration.

9. The machine must be flexible enough to enable the purchaser to add other document of similar shape (in case of passport machine – ID-3 size, and in case of ID card machine ID-1 size documents) including black-and-white laser engraving, colour photo creation with the same technology as it is offered for the documents from table #1, and quality control. In case of an ID card machine, it must be possible to perform coding both contact and contactless interfaces. The additional requirements are given below:

9.1. If the chip coding requires any add-on to be developed for the machine, it shall be possible in Java, C#, C++, Python or JavaScript programming language;

9.2. Laser engraving and photo creation shall be flexible to give the purchaser freedom of choose of desired layout for the visual elements;

9.3. Quality control shall support introduction of additional fonts;

9.4. It shall be possible selectively use visual personalization, chip coding, quality control or any combination of theml;

9.5. Documentation shall be supplied together with machines to let the purchaser introduce additional document types by its own resources.

4.9.4 Support and Maintenance requirements

1. To ensure high availability of the personalisation solution the Supplier must have locally based (in Georgia) support service with experience in identity and travel document technology support and maintenance. The support and maintenance contract shall last until PSDA prints the last blank supplied according to the contract drawn in the scope of this tender.
2. The Supplier shall provide web-based support portal where PSDA will register requests which are subject of the support and maintenance. Registration and commenting on the incident by PSDA personnel shall result confirmation email containing incident text and registration date and time to the person who registered the request.
3. During validity of the Contract, the Supplier shall be obliged to eliminate any established and reported defects (errors) of the personalisation solution free of charge.
4. During validity of the Contract, the Supplier shall be obliged to ensure free-of-charge preventive maintenance (according to the manufacturer's schedule) of delivered components, timely security patches for the delivered or developed software, as well as software operation only with those operating system (OS) versions that are supported by the OS developer (which have security patches available).
5. Initial priority shall be determined by PSDA based on the following matrix:

Impact	Urgency			
	Urgent	High	Medium	Low
On Agency	I Priority	I Priority	II Priority	III Priority
On Department	I Priority	II Priority	III Priority	IV Priority
On Group	II Priority	II Priority	III Priority	IV Priority
On User	III Priority	III Priority	IV Priority	IV Priority

6. Priority of each incident can be changed based on the mutual agreement between PSDA and the Supplier after signing the contract. The Supplier shall provide proper justification when requesting increase of the priority number (decreasing urgency and/or impact)
7. Response and resolution times shall be determined as follows. Maximum term for the resolution shall be counted starting from the incident registration:

Priority	Response action (reaction) term	Maximum term for the resolution	Support Availability

Priority 1	1 hour or less	No more than 6 hours	9:00-18:00 Tbilisi time
Priority 2	1 hour or less	No more than 12 hours	9:00-18:00 Tbilisi time
Priority 3	2 hours or less	No more than 1 working day	9:00-18:00 Tbilisi time, Monday - Friday
Priority 4	4 hours or less	No more than 3 working days	9:00-18:00 Tbilisi time, Monday – Friday

8. In case if the Supplier is unable to meet maximum service term given in the paragraph 7, it has right to request extension of the deadline, by providing motivated justification and time needed for the resolution. The explanation shall be presented before the end of the mentioned term and PSDA shall respond without the undue delay. In case if PSDA accepts the request, exceeding of the term will not be considered as a violation and the Supplier will not be a subject of penalties. Actions and terms for eliminating of the incidents will be defined based on mutual agreement.
9. For priority 1 and priority 2 incidents, PSDA shall have right to request support availability extension to 24 (twenty four) hours per day, for 60 (sixty) days per 1 (one) contract year (The year starting from the contract signature. For incomplete year, number of days shall be decreased proportionally to the available days). PSDA shall have right to request support availability extension for priority 1 incidents without any kind of prior agreements. The extension caused by the Supplier will not cause decrease of the number of days eligible for 24-hour support.
10. Failure of meeting the deadlines set in paragraph 7 will be a subject of penalties stipulated by the contract.

4.9.5 Personalization of graphical elements

4.9.5.1 Primary portrait personalization for both card and passport documents

1. The primary portrait of the bearer of the document shall be in colour. Base size of 40 (fourty) mm height and 30 (thirty) mm width shall be assumed, the exact size shall be agreed between the Supplier and PSDA,
2. The colour portrait shall be obtained during the personalization using laser engraving technology. It is not allowed to embed the portrait during polycarbonate body (eID card or ePassport data page) assembly. The following additional requirements apply:
   2.1. If the laser engraving results the colour picture, no more processing of the portrait (e.g. using inks in addition to the laser) shall happen;
   2.2. If the technology assumes creation of the black-and-white picture with laser, it shall be supplemented with the inks applied using the inkjet printer on the top of the polycarbonate surface in a way which results the colour picture, does not distract security features applied to the polycarbonate material during production, and guarantee visibility of the laser

engraved portrait in IR (infrared). Black inks shall not be used and all black parts shall be produced using the laser.

2.3. No protected overlay shall be applied after the portrait is printed. For the security and durability of the picture printing technology according to the paragraph 2.2, the printing process may assume using the inkjet printer to create the positive structures raised above the polycarbonate level only in case the following requirements are met:

2.3.1. These structures shall contain the surface relief;

2.3.2. The part raised above the polycarbonate layer shall be securely linked to the cardholder's portrait using level 1 and/or level 2 security feature(s);

2.3.3. The laser engraved portrait (see paragraph 2.2) shall be protected with the diffractive optically variable image device (DOVID) that is based on partial metallization technology, provides transparency using high definition (containing lines with 20μm or less thicknesses), contains Level 1, Level 2 and Level 3 security features and is positioned on a layer of the eID card and ePassport data page that is used for the laser engraving.

2.4. Regardless of the colour picture technology, the laser engraving step shall produce full face picture in the polycarbonate, with the resolution required by the present document (chapter 4.9.3, paragraph 1).

2.5. The offered technology of the portrait personalization, as well as additional security and durability measures (including measures to meet requirements of the chapter 2.3, if applicable) has to be clearly described to PSDA, containing the security concept which includes risk analysis by identifying potential threats and the proposed protection methods.

4.9.5.2 Other elements for the passport

1. The passport graphical personalization shall satisfy the following requirements:
   1.1. Conventional (black and white) laser engraving of text data and MRZ lines shall be done,
   1.2. Laser engraving of the transparent or/and semi-transparent structure and/or lenticular area (CLI, MLI or similar technologies) shall be done with the variable data,
   1.3. Microtext engraving shall not be higher than 200 μm with perfect registration on the datapage background printing,
   1.4. At least one graphic element shall be customized by raised tactile laser on the front of the document,
   1.5. 6 digits CAN (Card Access Number) shall be engraved on the front of the Datapage as specified by ICAO.
2. No overlay or glue shall be added to the structure and in particular no overlay shall be placed after the graphic personalization of the document,

4.9.5.3 Other elements for the card

1. The card graphical personalization shall satisfy the following requirements:
   1.1. Conventional (black and white) laser engraving of text data and MRZ lines shall be done,
   1.2. Laser engraving of the transparent or/and semi-transparent structure and/or lenticular area (CLI, MLI or similar technologies) shall done with the variable data,
   1.3. Microtext engraving shall not be higher than 200 µm, with perfect registration on the card background printing on the portrait side of the card,
   1.4. At least one graphic element shall be customized by raised tactile laser on the back of the document,
   1.5. 6 digits CAN (Card Access Number) shall be engraved on the front of the card as specified by ICAO.
2. No overlay or glue shall be added to the structure and in particular no overlay shall be placed after the graphic personalization of the document,

4.9.6 Off-machine Quality control

1. The off-machine quality control solution shall be delivered in the form of the software library (no source code is mandatory) which can be integrated in the personalization system developed by PSDA. Windows 7 or above shall be supported
2. The quality control solution shall support the following document scanners:
   2.1. Regula
   2.2. Crossmatch
3. The quality control functionality shall verify the content of electronic chips listed below:
   3.1. DGs (including DG3 after EAC)
   3.2. Access Control methods supported
      3.2.1. BAC,
      3.2.2. Terminal Authentication,
      3.2.3. PACE,
      3.2.4. Passive Authentication,
      3.2.5. Chip Authentication
      3.2.6. Active Authentication.
4. Verification of graphical elements:
      4.1.1. Biographic data,
      4.1.2. Signature,
      4.1.3. MRZ,
      4.1.4. IR and UV scanning.

4.9.7 Mail Finishers

1. PSDA requires supply mail finisher machines for creating laser-printed PIN/PUK mailers

2. Mail finisher shall be delivered in assembly with the general-purpose high performance laser printer (black and white) with network printing capability.
3. The mail finisher shall operate using the following principle:
   3.1. printer shall be capable of printing the received data on A4-sized pages (thermal glue will be pre-applied to each page);
   3.2. The printer shall securely pass the printed paper it to the sealer;
   3.3. The sealer shall 3-fold the resulting paper and seal it.

4.9.8 Inserting machines for envelopes

1. PSDA requires supply of inserting machines to automate the following processes
   1.1. Insertion of the PIN/PUK mailer in the envelope
   1.2. Folding of the A4-format papers and insertion them in the envelope
2. Envelopes of C6/5 (114mm x 229 mm) size shall be supported
3. The machines shall be capable to seal the envelopes or left them unsealed, according to operation mode chosen by the operator of the machine

4.10 Delivery of the security keys and other sensitive material

1. PSDA and the Supplier shall exchange the RSA-4096 public keys compatible with GPG with AES-256 content encryption key. PSDA will provide its public key after contract signing. At least security key exchange shall be encrypted and signed using these keys. The Supplier shall have right to encrypt and/or sign any other information with this key too.
2. All key material for encryption or integrity check of the electronic data shall be delivered to PSDA in encrypted form, using key-exchange-key (KEK).
3. If not otherwise agreed with the Supplier and PSDA in written form, the following requirements shall apply on KEK exchange:
   3.1. KEK shall be of 2TDEA, 3TDEA or AES type
   3.2. KEK shall be divided in 3 (three) parts in such a way the length of each part is same as the length of the final key, and calculation of the final key is only possible when all parts are known;
   3.3. Each part of KEK shall have control value (KCV). Also, the KEK itself shall have summary control value (KCV);
   3.4. Key division and KCV calculation algorithm shall be selected in a way which allows PSDA to load all keys in the Hardware Security Module (HSM) of type SafeNet ProtectServer External it operates, and use HSM's standard capabilities for combining key parts to the key, and to control KCV correctness;
   3.5. All parts (thirds) of all keys belonging to KEK shall be delivered to 3 different persons named by PSDA. The delivery shall happen in a material way, using sealed envelope which will be evident to the tampering. The delivery may happen face-to-face by the Supplier's representatives or by postal delivery;

3.6. Part of KEK shell not be sent to the addressee until the confirmation of reception is received from the addressee of the previous part;

4. All other keys shall be encrypted using KEK, and then encrypted using PSDA's GPG key exchanged according to the paragraph 1. The encrypted package shall be delivered to PSDA by email. Each key shall be encrypted in a way which will let PSDA to load these keys in Hardware Security Module (HSM) of type SafeNet ProtectServer External and unwrap them there, without exporting KEK outside of the HSM.