# ახალი თაობის პირადობის დამადასტურებელ დოკუმენტებთან დაკავშირებული მოთხოვნები

# 1 შესავალი

წინამდებარე დოკუმენტში სიტყვა „პასპორტის“ ან „ელექტრონული პასპორტის“ გამოყენებისას, დოკუმენტის ტიპის მკაფიოდ მითითების გარეშე, შესაბამისი მოთხოვნა შეეხება ყველა დოკუმენტს, რომელიც #1 ცხრილში აღნიშნულია, როგორც „TD-3“. ასევე, წინამდებარე დოკუმენტში სიტყვა „პირადობის ელექტრონული მოწმობის“ გამოყენებისას, დოკუმენტის ტიპის მკაფიოდ მითითების გარეშე, შესაბამისი მოთხოვნა შეეხება ყველა დოკუმენტს, რომელიც #1 ცხრილში აღნიშნულია, როგორც „TD-1“.

ცხრილი #1

| # | **შესყიდვის ობიექტის დასახელება** | **ფორმატი** | **რაოდენობა** |
|---|---|---|---|
| 1 | საქართველოს მოქალაქის ბიომეტრიული პასპორტის ბლანკი | TD-3 | 2 400 000 |
| 1.1 | საქართველოს მოქალაქის ბიომეტრიული პასპორტის ბლანკის ნიმუში | TD-3 | 2000 |
| 2 | საქართველოს მოქალაქის ბიომეტრიული დიპლომატიური პასპორტის ბლანკი | TD-3 | 7000 |
| 2.1 | საქართველოს მოქალაქის ბიომეტრიული დიპლომატიური პასპორტის ბლანკის ნიმუში | TD-3 | 1000 |
| 3 | საქართველოს მოქალაქის ბიომეტრიული სამსახურებრივი პასპორტის ბლანკი | TD-3 | 7000 |
| 3.1 | საქართველოს მოქალაქის ბიომეტრიული სამსახურებრივი პასპორტის ბლანკის ნიმუში | TD-3 | 1000 |
| 4 | საქართველოში სტატუსის მქონე მოქალაქეობის არმქონე პირის ბიომეტრიული სამგზავრო პასპორტის ბლანკი | TD-3 | 7000 |
| 4.1 | საქართველოში სტატუსის მქონე მოქალაქეობის არმქონე პირის ბიომეტრიული სამგზავრო პასპორტის ბლანკის ნიმუში | TD-3 | 1000 |
| 5 | ლტოლვილის ბიომეტრიული სამგზავრო დოკუმენტის ბლანკი | TD-3 | 7000 |

| | | | |
|---|---|---|---|
| 5.1 | ლტოლვილის ბიომეტრიული სამგზავრო დოკუმენტის ბლანკის ნიმუში | TD-3 | 1000 |
| 6 | ნეიტრალური სამგზავრო დოკუმენტის ბლანკი | TD-3 | 7000 |
| 6.1 | ნეიტრალური სამგზავრო დოკუმენტის ბლანკის ნიმუში | TD-3 | 1000 |
| 7 | ჰუმანიტარული სტატუსის მქონე პირის ბიომეტრიული სამგზავრო დოკუმენტის ბლანკი | TD-3 | 7000 |
| 7.1 | ჰუმანიტარული სტატუსის მქონე პირის ბიომეტრიული სამგზავრო დოკუმენტის ბლანკის ნიმუში | TD-3 | 1000 |
| 8 | თანამემამულის მოწმობის ბლანკი | TD-1 | 6500 |
| 8.1 | თანამემამულის მოწმობის ბლანკის ნიმუში | TD-1 | 1000 |
| 9 | პირადობის ელექტრონული მოწმობის ბლანკი | TD-1 | 3 500 000 |
| 9.1 | პირადობის ელექტრონული მოწმობის ბლანკის ნიმუში | TD-1 | 2000 |
| 10 | დროებითი ბინადრობის ელექტრონული მოწმობის ბლანკი | TD-1 | 150 000 |
| 10.1 | დროებითი ბინადრობის ელექტრონული მოწმობის ბლანკის ნიმუში | TD-1 | 1000 |
| 11 | მუდმივი ბინადრობის ელექტრონული მოწმობის ბლანკი | TD-1 | 30 000 |
| 11.1 | მუდმივი ბინადრობის ელექტრონული მოწმობის ბლანკის ნიმუში | TD-1 | 1000 |
| 12 | პირადობის ნეიტრალური მოწმობის ბლანკი ქართულ-ოსური | TD-1 | 7000 |
| 12.1 | პირადობის ნეიტრალური მოწმობის ბლანკის ნიმუში ქართულ-ოსური | TD-1 | 1000 |

| | | | |
|---|---|---|---|
| 13 | პირადობის ნეიტრალური მოწმობის ბლანკი ქართულ-აფხაზური | TD-1 | 7000 |
| 13.1 | პირადობის ნეიტრალური მოწმობის ბლანკის ნიმუში ქართულ-აფხაზური | TD-1 | 1000 |
| 14 | დროებითი საიდენტიფიკაციო მოწმობის ბლანკი | TD-1 | 7000 |
| 14.1 | დროებითი საიდენტიფიკაციო მოწმობის ბლანკის ნიმუში | TD-1 | 1000 |

## განმარტებები და ტერმინოლოგიის გამოყენება

1. **ეკვივალენტური სტანდარტი** - ეკვივალენტობა დგინდება საქართველოს კანონმდებლობის (მათ შორის პროდუქტის უსაფრთხოებისა და თავისუფალი მიმოქცევის კოდექსის) შესაბამისად. ამა თუ იმ სტანდარტის „ეკვივალენტური სტანდარტის“ დანიშნულებით გამოყენების პირველივე შემთხვევისას სააგენტოს უნდა მიეწოდოს მითითებები, საქართველოს კანონმდებლობის შესაბამის დებულებებზე, წარმოდგენილი სტანდარტის ეკვივალენტურობის დადასტურების მიზნით (მაგალითად, თუ ეკვივალენტური სტანდარტი გამოყენებულია სატენდერო წინადადებაში, აღნიშნული დებულებებზე მითითებები უნდა დაერთოს სატენდერო წინადადებას).
2. **ახალი სტანდარტი** - ახალი სტანდარტის გამოყენება დასაშვებია მხოლოდ იმ შემთხვევაში, თუ მას იგივე ორგანიზაცია გასცემს (რამდენიმე ორგანიზაციის შემთხვევაში, როგორიცაა ISO და IEC, სულ მცირე, ერთ-ერთი მათგანი) და დაცულია სულ მცირე ერთ-ერთი შემდეგი პირობა: ა) ახალ სტანდარტს აქვს იგივე ნომერი, ან ბ) მის ტექსტში ნათლადაა მითითებული, რომ ძველი სტანდარტი ჩაანაცვლა ახალმა. ამა თუ იმ სტანდარტის „ახალი სტანდარტის“ როლში გამოყენების პირველივე შემთხვევისთანავე სააგენტოს მტკიცებულების სახით უნდა მიეწოდოს შესაბამისი ამონარიდები ახალი სტანდარტიდან (მაგალითად, თუ ახალი სტანდარტი გამოყენებულია სატენდერო წინადადებაში, აღნიშნული ამონარიდები უნდა დაერთოს სატენდერო წინადადებას).
3. **დამამზადებელი საწარმო** - ადგილი (საწარმო), სადაც პროდუქტი (მაგალითად, დოკუმენტის ბლანკი) საბოლოო სახეს იძენს.

# 2 ინფორმაცია პრეტენდენტზე

პრეტენდენტმა უნდა დააკმაყოფილოს წინამდებარე დოკუმენტით განსაზღვრული მოთხოვნები. პრეტენდენტს უფლება აქვს, წინამდებარე დოკუმენტით განსაზღვრული წესით იყოლიოს დაკავშირებული კომპანიები (იხ. 2.5 თავი) და ქვეკონტრაქტორები.

სატენდერო წინადადება უნდა მოიცავდეს წინამდებარე თავითა და მისი ქვეთავებით მოთხოვნილ ინფორმაციასა და დოკუმენტაციას.

## 2.1 ნაწილი 1: ფინანსური მდგრადობა

აღნიშნული მოთხოვნები რეგულირდება სატენდერო დოკუმენტაციით

## 2.2 ნაწილი 2: გამოცდილება და რეკომენდაციები

აღნიშნული მოთხოვნები რეგულირდება სატენდერო დოკუმენტაციით

## 2.3 ნაწილი 3: ტექნიკური და პროფესიული შესაძლებლობები

1. შემოთავაზებული ელექტრონული ბლანკის ოპერაციული სისტემა/სისტემები, მათ შორის, eID, eMRTD და დამხმარე მონაცემთა აპლიკაციები, შემუშავებული უნდა იყოს პრეტენდენტის, მისი დაკავშირებული კომპანიის ან ქვეკონტრაქტორის მიერ (პირის სახელი მითითებული უნდა იყოს common criteria სერტიფიკატზე). პრეტენდენტი პასუხისმგებელია პროდუქტის უსაფრთხოებაზე. მან დროულად უნდა აცნობოს სააგენტოს გამოყენებულ პროდუქტებში შესაძლო და დადასტურებული სისუსტეების შესახებ და უზრუნველყოს სააგენტოსთვის აღნიშნული სისუსტეების პროგრამული აღმოფხვრა დაუსაბუთებელი შეფერხების გარეშე.

2. პრეტენდენტი იღებს ვალდებულებას, შეიმუშავოს რისკის ანალიზისა და რისკის მართვის გეგმა, რომელიც ითვალისწინებს პროექტთან დაკავშირებულ რისკებზე რეაგირებას და ბიზნესის უწყვეტობის უზრუნველყოფას ფორსმაჟორული გარემოების შემთხვევაში, რათა კონტრაქტით ნაკისრი ვალდებულებების შესრულება (შეფერხების შემთხვევაში) განახლდეს მაქსიმალურად მოკლე დროში. ხსენებული დოკუმენტები, ხელშეკრულების მოქმედების მთელი პერიოდის მანძილზე, უნდა ექვემდებარებოდეს მიმწოდებლის მხრიდან მუდმივ რევიზიასა და არსებულ რეალობასთან შესაბამისობის უზრუნველყოფას. სააგენტო უფლებამოსილია, ნებისმიერ ეტაპზე გადაამოწმოს აღნიშნული ვალდებულების შესრულება მისთვის სასურველი ნებისმიერი ფორმით, მათ შორის წინამდებარე დოკუმენტის 4.8 თავის შესაბამისად განსაზღვრული წესითაც.
3. შემოთავაზებული მიკროსქემის მწარმოებელს თავისი მიკროსქემის პროდუქტები ინტეგრირებული უნდა ჰქონდეს პირადობის დამადასტურებელი და სამგზავრო დოკუმენტის ოპერაციული სისტემისა და აპლიკაციის, სულ მცირე, 3 სხვადასხვა დეველოპერთან (მიმწოდებლებთან) და უნდა ფლობდეს თავის სახელზე რეგისტრირებულ Common Criteria (EAL 5+ ან უფრო მაღალი დონის), სულ მცირე, 20 სერტიფიკატს (რომლებიც ადასტურებენ, რომ იგი გამოყენებულ იქნა, როგორც პლატფორმა საიდენტიფიკაციო ან სამგზავრო დოკუმენტების ოპერაციული სისტემებისა და აპლიკაციებისათვის). სატენდერო წინადადება უნდა შეიცავდეს სერტიფიკატებს.
4. სატენდერო წინადადების განთავსებით პრეტენდენტი ადასტურებს, რომ მისთვის ცნობილია „მკაცრი აღრიცხვის ფორმების შესახებ“ საქართველოს კანონი

(https://matsne.gov.ge/en/document/view/30946) და იღებს პასუხისმგებლობას, ხელშეკრულების გაფორმების შემთხვევაში, სრულად დააკმაყოფილოს აღნიშნული კანონის მოთხოვნები ხელშეკრულების მოქმედების მთელი ვადის განმავლობაში (კანონში ცვლილებების ჩათვლით).

5. ყველა სხვა მოთხოვნა ტექნიკური და პროფესიული შესაძლებლობების მიმართ რეგულირდება სატენდერო დოკუმენტაციით

## 2.4 ნაწილი 4: შემოთავაზებული ბლანკებისა და სხვა კომპონენტების დეტალები

აღნიშნული მოთხოვნები რეგულირდება სატენდერო დოკუმენტაციით

## 2.5 ნაწილი 5: პრეტენდენტთან დაკავშირებული კომპანიები

1. პრეტენდენტს უფლება აქვს, დაეყრდნოს დაკავშირებული კომპანიების გამოცდილებას და ამ მიზნით წინამდებარე დოკუმენტით განსაზღვრული დასაშვებობის კრიტერიუმების დამადასტურებლად წარმოადგინოს დაკავშირებული კომპანიის/კომპანიების მიმართ გაცემული დოკუმენტაცია.
2. სატენდერო წინადადებას უნდა დაერთოს თითოეული იმ დაკავშირებული კომპანიის დასტური პროექტში ჩართვასთან დაკავშირებით (დაკავშირებული კომპანია უნდა ჩაერთოს პროექტის იმ ნაწილში, სადაც პრეტენდენტს გამოცდილება არ აქვს მე-2 თავის მიხედვით, ხელშეკრულების მოქმედების მთელი პერიოდის განმავლობაში), რომელსაც უთითებს ან რომლის მაჩვენებლებსაც ეყრდნობა პრეტენდენტი. დაკავშირებული კომპანია შეიძლება იყოს:
   2.1. პრეტენდენტის შვილობილი კომპანია;
   2.2. პრეტენდენტის ფილიალი;
   2.3. პრეტენდენტის მშობელი კომპანია;
   2.4. პრეტენდენტის მშობელი კომპანიის შვილობილი კომპანია.
3. სატენდერო წინადადებას უნდა დაერთოს დოკუმენტაცია, რომელიც დაადასტურებს მე-2 პუნქტის მითითებული იერარქიას და ცხადად აჩვენებს თითოეული მშობელი კომპანიის მირ თითოეულ შვილობილ კომპანიაში წილის ფლობას. თუ რომელიმე მშობელი კომპანიის წილი რომელიმე შვილობილ კომპანიაში 100% არ არის, სატენდერო წინადადებას ასევე უნდა დაერთოს დიდ ოთხეულში შემავალი აუდიტორული კომპანიის (PricewaterhouseCoopers, Deloitte Touche Tohmatsu, Ernst & Young, KPMG) დასკვნა, რომელშიც მკაფიოდ იქნება მითითებული რომ მშობელ კომპანიას ეკუთვნის შვილობილი კომპანიის წილის საკონტროლო პაკეტი.
4. თუ დაკავშირებულ კომპანიად წარმოდგენილია პრეტენდენტის მშობელი კომპანიის შვილობილი კომპანია, სავალდებულოა ეს მშობელი კომპანია ორივე შვილობილთან

(პრეტენდენტი და დაკავშირებული კომპანია) მიმართებაში აკმაყოფილებდეს დაკავშირებული კომპანიისადმი ამ თავის მე-3 პუნქტით დაწესებულ ყველა მოთხოვნას - მიუხედავად იმისა, სატენდერო წინადადებაში თავად მშობელი კომპანია წარმოდგენილი იქნება თუ არა დაკავშირებულ კომპანიად.

5. მე-4 პუნქტის დასაკმაყოფილებლად წარმოდგენილი დოკუმენტაცია უნდა ადასტურებდეს 100% წილის ფლობას ან/და საკონტროლო პაკეტის ფლობას თითოეული მშობელი-შვილობილი კომპანიის შემთხვევაში უწყვეტად 6 თვის განმავლობაში ტენდერის გამოცხადების მომენტამდე.
6. წინამდებარე ტენდერის ფარგლებში დაკავშირებულ კომპანიებად ჩაითვლებიან მხოლოდ ის კომპანიები, რომელთა შესახებ ინფორმაცია მოწოდებული იქნება სატენდერო წინადადებაში წინამდებარე თავის მოთხოვნათა სრული დაცვით. სხვა კომპანიები, მიუხედავად პრეტენდენტთან მათი სამართლებრივი ურთიერთობის ფორმისა, არ დაექვემდებარებიან განხილვასა და შეფასებას.

# 3 ხელშეკრულების შესრულება

## 3.1 ზოგადი მოთხოვნები პროექტის მართვისა და სააგენტოსთან თანამშრომლობის მიმართ

1. სასტარტო შეხვედრა ტარდება ხელშეკრულების ხელმოწერის შემდეგ. სააგენტოს წარედგინება მომწოდებლის პერსონალი (ვინც ჩართული იქნება კონტრაქტის განხორციელების პროცესში), კერძოდ, პროექტის და ქვეპროექტის მენეჯერები (მაგ., დოკუმენტის ბლანკის წარმოებისათვის, ჩაშენებული ელექტრონული კომპონენტებისთვის, შუალედური პროგრამული უზრუნველყოფისა და სისტემებისათვის), დოკუმენტის ბლანკის დიზაინერი, სისტემური არქიტექტორი და პროგრამული უზრუნველყოფის დეველოპერები.
2. სასტარტო შეხვედრაზე განიხილება ზოგადი საპროექტო გეგმა.
3. სააგენტოს უნდა მიეცეს, სულ მცირე, 10 (ათი) სამუშაო დღის ვადა (საქართველოს კანონმდებლობით დადგენილი უქმე დღეების გამოკლებით) წინამდებარე შესყიდვის ფარგლებში საქონლის და მომსახურების მიღების დასადასტურებლად ან მასზე უარის სათქმელად.
4. კონტრაქტის მოქმედების ვადის განმავლობაში მომწოდებელმა უნდა იქონიოს რეგულარული კომუნიკაცია სააგენტოსთან.
5. მომწოდებლის პროექტის მენეჯერი ვალდებულია, კვირაში ერთხელ წარუდგინოს სააგენტოს პროექტის მენეჯერს საინფორმაციო ანგარიში, სააგენტოსთან შეთანხმებული პროექტის მართვის მეთოდოლოგიის შესაბამისად.
6. უნდა შეიქმნას პროექტის მმართველი კომიტეტი, რომლის წევრებიც იქნებიან ორივე მხარის პროექტის მენეჯერები და მაღალი მენეჯერული რგოლის წარმომადგენლები (აღმასრულებელი დირექტორები ან/და თავმჯდომარეები, მათი მოადგილეები და სხვ.). მმართველი კომიტეტი ზედამხედველობას გაუწევს პროექტის განხორციელების პროცესს.
7. სააგენტოს მოთხოვნის შემთხვევაში, მომწოდებელი ვალდებულია, დააფუძნოს ადგილობრივი წარმომადგენლობა საქართველოში.

## 3.2 კონტრაქტის ბიჯები და ეტაპები

1. მომწოდებელი ვალდებულია, წარუდგინოს სააგენტოს ელექტრონული პასპორტის დამზადებისათვის საჭირო პერსონალიზაციის აღჭურვილობის, სულ მცირე ერთი კომპლექტი კონტრაქტის გაფორმებიდან არაუგვიანეს 6 (ექვსი) თვის ვადაში, ხოლო პერსონალიზაციის მანქანების გაფართოებების შემუშავებისა და ტესტირებისათვის საჭირო აპარატურა, ასევე მანქანის გარეთ ხარისხის კონტროლის ბიბლიოთეკა - კონტრაქტის გაფორმებიდან არაუგვიანეს 3 (სამი) თვის ვადაში. წინამდებარე დოკუმენტით განსაზღვრული პერსონალიზაციის აღჭურვილობა სააგენტოს უნდა მიეწოდოს კონტრაქტის გაფორმებიდან არაუგვიანეს 7 (შვიდი) თვის განმავლობაში.

2. მომწოდებელი ვალდებულია, კონტრაქტის გაფორმებიდან არაუგვიანეს 6 (ექვსი) თვეში მიაწოდოს სააგენტოს ელექტრონული პასპორტის 500 (ხუთასი) სატესტო ბლანკი და პირადობის ელექტრონული მოწმობის 500 (ხუთასი) სატესტო ბლანკი, რომლებიც შეიძლება გამოყენებულ იქნეს პერსონალიზაციის პროგრამული გადაწყვეტის საწყისი ტესტირებისთვის. სატესტო ბლანკები სააგენტოს გადაეცემა უსასყიდლოდ.

3. მომწოდებელი სააგენტოს უნდა წარუდგინოს ელექტრონული პირადობის მოწმობისა და ელექტრონული პასპორტის ჩაშენებული პროგრამული უზრუნველყოფის (IAS და eMRTD აპლიკაციების) უსაფრთხოების სერტიფიკატების ასლები კონტრაქტის გაფორმებიდან არაუგვიანეს 14 (თოთხმეტი) თვის განმავლობაში. აღნიშნული უსაფრთხოების სერტიფიკატები გაცემული უნდა იყოს SOG-IS-ის შეთანხმების წევრი სერტიფიცირების ორგანოს მიერ (www.sogis.org).

4. მომწოდებელმა სააგენტოს უნდა წარუდგინოს ელექტრონული პირადობის მოწმობისა და ელექტრონული პასპორტისათვის შეთავაზებული ჩაშენებული პროგრამული უზრუნველყოფის ფუნქციური ტესტირების ანგარიშები, რომლებიც მიიღება აღიარებული კომპლექსური ტესტების რედაქტორის მიერ შემუშავებული ტესტირების ინსტრუმენტის მეშვეობით. წარდგენა ელექტრონული პასპორტისათვის უნდა მოხდეს კონტრაქტის გაფორმებიდან არაუგვიანეს 6 (ექვსი) თვის, ხოლო ელექტრონული პირადობის მოწმობისათვის არაუგვიანეს 10 (ათი) თვის ვადაში.

5. კონტრაქტის გაფორმებიდან არაუგვიანეს 6 (ექვსი) თვის განმავლობაში სააგენტოს უნდა მიეწოდოს პირადობის ელექტრონული მოწმობის შუალედური პროგრამული უზრუნველყოფა (4.7 თავის შესაბამისად).

6. მომწოდებელმა სააგენტოს უნდა მიაწოდოს ბლანკები დანართში მითითებული მიწოდების გრაფიკის შესაბამისად.

7. მომწოდებელი ვალდებულია, ყველა ბლანკის დიზაინი შეუთანხმოს შემსყიდველს კონტრაქტის გაფორმებიდან 3 (სამი) თვის ვადაში (შემსყიდველის შესაბამისი წარმომადგენელი მიმწოდებლისთვის დისტანციურად ხელმისაწვდომი იქნება სამუშაო საათების (საქართველოს დროით) განმავლობაში ხელშეკრულების გაფორმების მომდევნო დღიდან). შემსყიდველის წარმომადგენლის მხრიდან მიმწოდებლის მიერ გადმოგზავნილ შესათანხმებელ საკითხებზე ყოველ კონკრეტულ შემთხვევაში 3 (სამი) სამუშაო დღეს გადაცილებული დღეების საერთო ჯამური რაოდენობა ემატება ზემოაღნიშნულ სამთვიან ვადას. შემსყიდველი პასუხისმგებელია მოსაწოდებელი ბლანკის საბოლოო დიზაინის დადასტურებასა და შესაბამის ნორმატიულ აქტებში ცვლილების განხორციელებაზე. მიმწოდებელი კისრულობს პასუხისმგებლობას შემსყიდველთან შეთანხმებულ ბლანკის დაცვის ელემენტებთან დაკავშირებით საავტორო უფლებების დარღვევის გამო მესამე მხარეების მიერ წარმოდგენილი პრეტენზიებისთვის (გარდა თავად სააგენტოს მიერ შემოთავაზებული დიზაინის ელემენტებისა).

8. მომწოდებელმა უნდა მოამზადოს #1 ცხრილში მოყვანილი ყველა პასპორტისა და პირადობის მოწმობისათვის სრულყოფილი დოკუმენტის ნიმუში და მიაწოდოს შემსყიდველს ფინანსთა სამინისტროში რეგისტრაციისათვის არაუგვიანეს 1 (ერთი) თვის ვადაში მას შემდეგ, რაც სააგენტო მომწოდებელს აცნობებს წინამდებარე დოკუმენტით გათვალისწინებული შესაბამისი ნორმატიული აქტის (ბლანკის ფორმის დამტკიცების შესახებ საქართველოს იუსტიციის მინისტრის ბრძანება) დამტკიცების შესახებ.

9. მომწოდებელმა უნდა დაამტკიცოს, რომ მას შეუძლია აწარმოოს ბლანკები წინამდებარე ტენდერით განსაზღვრული ხარისხის მოთხოვნების (წინამდებარე დოკუმენტის 4.2 თავის) შესაბამისად. აღნიშნული მტკიცებულებები, 4.2 თავის შესაბამისად, უნდა წარედგინოს სააგენტოს, წინამდებარე თავის მე-8 პუნქტის თანახმად წარმოდგენილი ბლანკების მიწოდებიდან არაუგვიანეს 1 (ერთი) თვეში. იმავე ვადის განმავლობაში მიწოდებულ უნდა იქნეს შესაბამისი დოკუმენტების ნორმალური მოხმარების პირობები.

10. შემსყიდველი პასუხისმგებელია დოკუმენტის ბლანკების რეგისტრაციასა და სარეგისტრაციო იდენტიფიკატორების მიღებაზე სარეგისტრაციო ნიმუშების მიღებიდან 2 (ორი) კვირის ვადაში. მომწოდებლისთვის აღნიშნული იდენტიფიკატორების მიწოდების შემდეგ მომწოდებელი ვალდებულია, დაბეჭდოს TD-3 ფორმატის დოკუმენტები, რომლებიც #1 ცხრილში აღნიშნულია, როგორც „ნიმუში“, ამავე ცხრილში მითითებული რაოდენობით და მიაწოდოს ისინი შემსყიდველს 2 (ორი) კვირის განმავლობაში. დოკუმენტები უნდა შეიცავდნენ შემსყიდველის მიერ მიწოდებულ იდენტიფიკატორებს.

11. ალგორითმი და პროგრამული უზრუნველყოფის მოდულები დოკუმენტის მფლობელის ფოტოსურათის ავტომატური ავთენტიფიკაციისათვის (წინამდებარე დოკუმენტის 4.4. თავის მე-5 პუნქტის თამახმად) სააგენტოს უნდა მიეწოდოს კონტრაქტის გაფორმებიდან არაუგვიანეს 6 (ექვსი) თვის ვადაში.

12. კონტრაქტის გაფორმებიდან არაუგვიანეს 24 (ოცდაოთხი) თვის განმავლობაში მომწოდებელმა უნდა დაიწყოს სააგენტოსათვის პირადობის ელექტრონული მოწმობების მიწოდება, რომლებშიც ჩაშენებული იქნება დამხმარე მონაცემების აპლიკაცია. თუ აღნიშნული გამოიწვევს ცვლილებებს IAS აპლიკაციაში (მაგ. Single Sign On შესაძლელობის შეტანის გამო), სააგენტოს უნდა მიეწოდოს შესაბამისი სერტიფიკატი არაუგვიანეს იმ ვადისა, რა ვადაშიც სააგენტოს მიეწოდება მოწმობები ახალი IAS აპლიკაციით. უსაფრთხოების სერტიფიკატი გაცემული უნდა იყოს SOG-IS-ის შეთანხმების წევრი სერტიფიცირების ორგანოს მიერ (www.sogis.org).

13. მომწოდებელმა სააგენტოს ყოველგვარი დამატებითი ხარჯისა და ღირებულების გარეშე უნდა მიაწოდოს ბლანკებზე არსებული მეორე დონის დამცავი ნიშნების შესამოწმებელი სპეციალური მოწყობილობების მინიმუმ, 10 (ათი) კომპლექტი, სადაც თითოეული კომპლექტი უნდა შედგებოდეს ერთი ან მეტი მოწყობილობისგან, რომლებიც ერთობლივად იძლევიან ყველა დამცავი ნიშნის შემოწმების საშუალებას. მიწოდება უნდა მოხდეს შესყიდვის ობიექტის (ბლანკების) პირველ მიწოდებამდე არაუგვიანეს 1 (ერთი) თვისა.

14. წინამდებარე თავით განსაზღვრული ვადების დარღვევა გამოიწვევს ხელშეკრულებით განსაზღვრული ჯარიმების დაკისრებას.

# 4 ტექნიკური მოთხოვნები

## 4.1 ზოგადი მოთხოვნები

1. პირადობის ელექტრონული მოწმობისა და ელექტრონული პასპორტის ბლანკების მონაცემთა გვერდები (გარდა თამასისა) დამზადებული უნდა იყოს 100%-იანი პოლიკარბონატისგან, რომელზეც შესაძლებელი იქნება ლაზერული გრავირების ტექნოლოგიის გამოყენება მათი პერსონალიზაციის მიზნებისთვის საქართველოში არსებულ სააგენტოს სამ პერსონალიზაციის ცენტრში, შემსყიდველის მიერ შემუშავებული პერსონალიზაციის სისტემის მეშვეობით.

2. პერსონალიზებულ დოკუმენტებში არ უნდა იყოს გამოყენებული ის დამცავი ნიშნები და მეთოდები, რომელთა მაღალხარისხიანი გაყალბებაც მოხდა.

3. ბლანკების დამცავი ნიშნების შემუშავებისა და მათი ბლანკზე დატანის დროს ფართოდ ხელმისაწვდომი სტანდარტული პროგრამული უზრუნველყოფის ინსტრუმენტები შეიძლება გამოყენებულ იქნეს შემუშავების მხოლოდ ადრეულ ეტაპზე. დამცავი ნიშნების შემუშავებისა და ბლანკზე დატანის პროცესების ფინალურ ეტაპზე აღნიშნული სტანდარტული ინსტრუმენტები უნდა შეივსოს ან შეიცვალოს შეზღუდული წვდომის სპეციალიზებული ინსტრუმენტებით.

4. შემოთავაზებული დამცავი ნიშნები ბლანკზე ისე უნდა იყოს განთავსებული, რომ ავსებდნენ და აერთიანებდნენ ერთმანეთს (ინტეგრირებული იყოს ერთმანეთთან) და, ამავდროულად, არ უშლიდნენ ხელს თითოეული ელემენტის ცალ-ცალკე შემოწმებას.

5. შემოთავაზებულმა ტექნოლოგიებმა უნდა უზრუნველყონ ხანგრძლივი დაცვა პერსონალიზაციის აღჭურვილობის, მათ შორის, ლაზერული გრავირების აპარატების გაზრდილი ხელმისაწვდომობით გამოწვეული საფრთხეებისგან (დიდი რაოდენობით მიწოდება, ფასის შემცირება, მათ შეძენაზე შეზღუდვების არარსებობა).

6. კონტრაქტი უნდა მოიცავდეს დოკუმენტის თითოეული ტიპისათვის ვიზუალური დიზაინისა და დამცავი ნიშნების ერთჯერადი განახლების ხარჯებს იმის გათვალისწინებით, რომ არსებული დამცავი ნიშნები შეიცვლება ახალი დამცავი ნიშნებით, რომელთა დაცვის სიძლიერე არანაკლებია განახლებამდე არსებული დამცავი ნიშნების სიძლიერისა ხელშეკრულების გაფორმების დროს. სააგენტომ მიმწოდებელს უნდა აცნობოს განახლებული დოკუმენტების დაგეგმილი გამოშვების თარიღამდე, სულ მცირე, 1 (ერთი) წლით ადრე.

7. კონტრაქტის გაფორმების შემთხვევაში მომწოდებელს არ შეუძლია, კონტრაქტის შესრულების დროს არგუმენტად მოიყვანოს გამოსაყენებელი ტექნოლოგიების შეზღუდვები, მაგალითად,

ცდომილება, ზომები, ხელმისაწვდომი ფერთა სპექტრი და სხვ., რომლებიც არ იყო ნახსენები ტექნიკურ წინადადებაში სატენდერო შეთავაზების წარდგენის დროს.

8. კონტრაქტის ვადის ამოწურვიდან არაუგვიანეს 6 (ექვსი) თვის განმავლობაში მომწოდებელმა სააგენტოს მეთვალყურეობის ქვეშ უნდა გაანადგუროს ბლანკების დამზადებისათვის საჭირო ყველა საბეჭდი ფილა, ლამინირების ფილა და პროექტისათვის სპეციფიკური სხვა მასალები, რაც ბლანკების წარმოებისათვისაა აუცილებელი. აღნიშნული ვალდებულება ასევე ვრცელდება პროექტისთვის სპეციფიკურ, ბლანკების წარმოებისათვის აუცილებელ ძველ მასალებზე, ამ თავის მე-6 პუნქტით განსაზღვრული განახლების შემთხვევაში.

## 4.2 მოთხოვნები გამძლეობის მიმართ

1. ელექტრონული პასპორტის ბლანკის საექსპლუატაციო ვადა უნდა შეადგენდეს, სულ მცირე, 10 (ათი) წელს. ამ მოთხოვნის დაკმაყოფილების მიზნით, უნდა ჩატარდეს ტესტირება პასპორტის ბლანკების საკმარის რაოდენობაზე, ქვემოთ მოყვანილი რომელიმე სტანდარტის შესაბამისად (ბლანკებმა წარმატებით უნდა გაიარონ „მინიმალური დონის სატესტო გეგმა“ მაინც):
   1.1. ICAO TR DURABILITY OF MACHINE READABLE PASSPORTS v3.2;
   1.2. ISO/IEC 18745-1.:2018 ან უფრო ახალი.

2. პირადობის ელექტრონული მოწმობის დიზაინი უნდა შეიქმნას ISO/IEC 24789-1-ის შესაბამისად, ხანდაზმულობის მე-3 კლასის და გამოყენების D კლასის გათვალისწინებით. ამ მოთხოვნის დაკმაყოფილების მიზნით, უნდა ჩატარდეს ტესტირება პასპორტის ბლანკების საკმარის რაოდენობაზე, ISO/IEC 24789-2-ის შესაბამისად.

3. ტესტირება უნდა ჩატარდეს ISO/IEC 17025 სტანდარტის შესაბამისად აკრედიტებული ლაბორატორიის მიერ. წარმოდგენილ უნდა იქნეს ლაბორატორიის აკრედიტაციის სერტიფიკატი და მასში ჩამოთვლილი უნდა იყოს შესაბამისი აკრედიტაციის სფერო (ICAO TR, ISO/IEC 18745-1, ISO/IEC 24789-2 - რომელიც გამოყენებულია).

4. თუ ძირითადი ფოტოსურათის პერსონალიზაციის ტექნოლოგია არ მოიცავს მხოლოდ ლაზერულ ამოტვიფვრას და პოლიკარბონატის ზედაპირზე მელნის დატანასაც გულისხმობს, უნდა დაკმაყოფილდეს შემდეგი მოთხოვნებიც:
   4.1. წინამდებარე თავში ნახსენები ყველა ტესტირება უნდა ჩატარდეს პირადობის ელექტრონულ მოწმობებსა და ელექტრონულ პასპორტებზე, რომლებზეც უკვე დატანილია პერსონალიზებული ძირითადი ფოტოსურათები, და უნდა დადასტურდეს, რომ ის ადგილები, რომელთა ფერადი პერსონალიზაციაც განხორციელდა, არ არის იმაზე ნაკლებად გამძლე, ვიდრე ის ნაწილები, რომლებიც მხოლოდ პოლიკარბონატისაა.

4.2. ადამიანის კანთან შეხება (მათ შორის, ცხიმთან შეხება) აღნიშნული ტექნოლოგიით დაცული ადგილების ნორმალურ ექსპლუატაციად ჩაითვლება.

5. შეთავაზებული ელექტრონული პასპორტების ბლანკების გამძლეობის ტესტირება (წინამდებარე თავის პირველი პუნქტის თანახმად) ასევე უნდა მოიცავდეს თამასის ტექნოლოგიის შემოწმებასაც, მათ შორის და არა მარტო, ფურცლის გამოქაჩვის, დელამინაციისა და ყველა თერმულ და ქიმიურ ტესტს.

6. წინამდებარე თავში განსაზღვრული ელექტრონული პასპორტისა და პირადობის ელეტრონული მოწმობის გამძლეობის ტესტები უნდა ჩატარდეს ჩაშენებული ჩიპის შემოთავაზებული მოდელისა და ელექტრონული კონფიგურაციის გამოყენებით (იგივე მოდელი, კავშირის ანტენის იგივე ტიპი და კონტაქტური დაფის მქონე პირადობის ელექტრონული მოწმობები) და წინამდებარე თავით განსაზღვრული მოთხოვნების შესაბამისად გამძლეობის ტესტის ჩატარების შემდეგ უნდა დამოწმდეს, რომ ელექტრონული კომპონენტები ისევ გამართულად მუშაობენ.

## 4.3 ელექტრონული პასპორტის სტრუქტურა და ფიზიკური დამცავი ნიშნები

1. ამ ნაწილში მოცემული მოთხოვნები ვრცელდება #1 ცხრილში მითითებულ ყველა ტიპის ელექტრონული პასპორტის (TD-3) ბლანკზე.

2. ყველა პასპორტის ფორმატი უნდა შეესაბამებოდეს ICAO 9303 სტანდარტს.

3. პასპორტის ექსპლუატაციის ვადა უნდა იყოს 10 (ათი) წელი.

4. ბუკლეტი უნდა შეიცავდეს:
   4.1. 48 (ორმოცდარვა) ქაღალდის გვერდს (შიდა გვერდი) და 1 (ერთი) ელექტრონულ ორგვერდიან, პოლიკარბონატისგან დამზადებულ ჩანართს (მონაცემთა გვერდი).
   4.2. მონაცემთა გვერდს, რომელსაც უნდა ჰქონდეს TD-3 ფორმატის პირადობის დამადასტურებელი დოკუმენტების სტანდარტებში მითითებული ფიზიკური მახასიათებლები, სიგრძით 125 მმ., სიგანით 88 მმ. და მონაცემთა გვერდის მაქსიმალური სისქით 0,9 მმ.
5. ბუკლეტი შედგება შემდეგი ელემენტებისგან:
   5.1. ყდა;
   5.2. ყდის შიდა გვერდები (ბოლო გვერდები);

5.3. შიდა გვერდები;
5.4. ელექტრონულ მონაცემთა გვერდი.

6. ბოლო გვერდების, შიდა გვერდებისა და ყდის გრაფიკული დიზაინი უნდა ინარჩუნებდეს ამჟამად არსებული საქართველოს პასპორტის დიზაინის მთავარ ელემენტებს, მაგრამ ასევე უნდა შეიცავდეს ცვლილებებსაც ბოლო და შიდა გვერდებზე, რაც გამყალბებლებს ხელს შეუშლის არსებული (მოპარული, დაკარგული და სხვ.) პასპორტების ელემენტების ხელმეორედ გამოყენებაში მაღალი ხარისხის ყალბი დოკუმენტების დამზადებისას. ამჟამად არსებული პასპორტის ბლანკის გრაფიკული დიზაინი მოცემულია დანართის სახით. რაც შეეხება გრაფიკულ დიზაინში არსებულ დამცავ ნიშნებს, მომწოდებელი არ არის შეზღუდული არსებული გრაფიკული დიზაინის ჩარჩოთი, განსაკუთრებით, მონაცემთა გვერდის მიმართ.

### 4.3.1 ყდა

1. წინამდებარე თავით განსაზღვრული მოთხოვნები მოქმედებს #1 ცხრილში მოცემული ყველა ელექტრონული პასპორტის მიმართ.

2. გარე ყდა უნდა იყოს დამზადებული 10-13 pts სისქის, 100%-იანი აკრილით დაფარული, ლატექსით გაჟღენთილი მასალისგან. ის უნდა უძლებდეს 175-185 გრადუს (ცელსიუსი) ტემპერატურაზე ლამინირებას. უნდა შეესაბამებოდეს პასპორტის შიდა ნაწილის ბოლო გვერდების მაღალი ხარისხის ლამინირებას.

3. გარეთა ნიშნები (მაგ., გერბი, წარწერები და ბლანკის ნიშანი დიზაინის მიხედვით) დატანილ უნდა იქნეს მაღალი ტემპერატურისა და წნევის ქვეშ (hot stamping), ოქროსფერი ლენტების გამოყენებით (სამრეწველო ოქრო), სუფთად გამოსახული კონტურებით და ხილული დეფექტების გარეშე.

4. წარწერები გარკვევით უნდა იყოს დატანილი და ადვილად უნდა იკითხებოდეს; მაღალი ტემპერატურისა და წნევის ქვეშ დატანილი წარწერები და ელემენტები უნდა იყოს ცვეთამედეგი და ჰქონდეს მუდმივი ბზინვარება.

5. ყდის ფერისათვის მიმწოდებელმა უნდა გამოიყენოს შემსყიდველთან შეთანხმებული ფერთა პალიტრა. შეთანხმება მოხდება წინამდებარე ტექნიკური დოკუმენტაციით განსაზღვრული წესით. ყოველი ბლანკის ყდის ფერი და დიზაინის ფაილები ტენდერში გამარჯვებულ კომპანიას გადაეცემა ხელშეკრულების დადების შემდეგ.

### 4.3.2 ყდის შიდა გვერდები

1. ამ პუნქტის მოთხოვნები მოქმედებს #1 ცხრილით განსაზღვრულ ყველა პასპორტის ბუკლეტთან მიმართ.

2. ყდის შიდა გვერდები დამზადებული უნდა იყოს მასალისგან, რომელიც არ ისრუტავს ან ირეკლავს ინფრაწითელ გამოსხივებას და რომლის წონა არის 120-140 გ. კვადრატულ მეტრზე (+/- 5% დასაშვები ცდომილებით). ქაღალდი უნდა დამზადდეს თეთრი ცელულოზისგან და, მინიმუმ, 50% ბამბისგან.

3. ნივთიერების ძირითადი მასალა უნდა იყოს ულტრაიისფერი სხივებისადმი მედეგი, სხვაგვარად - „ულტრაიისფერისადმი ყრუ“.

4. ყდის შიდა გვერდები უნდა შეიცავდეს:
   4.1. ძირითად ორნამენტს;
   4.2. ფარულ გამოსახულებას;
   4.3. ტექსტს;
   4.4. მიკროტექსტს ღრმა ბეჭდვის დიზაინით (ინტაგლიო), რომელიც მოიცავს ორ ან მეტ ფერს.

5. თითოეული ყდის შიდა გვერდი უნდა შეესაბამებოდეს ICAO-ს ნორმებს და უნდა შეიცავდეს, სულ მცირე, ქვემოთ ჩამოთვლილ დამცავ ელემენტებს:
   5.1. სარწმუნო ფონი (მიკროასოებით ბეჭდვა, გილიოშირება, ნუმიზმატური ნახატები, განზრახ დაშვებული შეცდომები);
   5.2. IR-split;
   5.3. 4 (ოთხი) პირდაპირი ტონის შემცველი, ინფრაწითელ სპექტრში უხილავი გამოსახულება, შესრულებული ოფსეტური ბეჭდვით;
   5.4. 1 (ერთი) უხილავი ულტრაიისფერი გამოსახულება შესრულებული ოფსეტური ბეჭდვით;
   5.5. მიკრობეჭდვა;
   5.6. ანტისკანირების დიზაინი.

### 4.3.3 პასპორტის შიდა გვერდები

1. ამ პუნქტის მოთხოვნები მოქმედებს #1 ცხრილში მითითებული ყველა პასპორტის ბლანკის მიმართ.

2. შიდა გვერდები დამზადებული უნდა იყოს მასალისგან, რომელიც არ ისრუტავს ან ირეკლავს ინფრაწითელ გამოსხივებას და რომლის წონა არის 90 გ. კვადრატულ მეტრზე (+/- 5% დასაშვები ცდომილებით).

3. ნივთიერების ძირითადი მასალა უნდა იყოს ულტრაიისფერი სხივებისადმი მედეგი, სხვაგვარად - „ულტრაიისფერისადმი ყრუ“.

4. ქაღალდი უნდა შედგებოდეს ხის მერქნისგან და, მინიმუმ, 50% ბამბისგან. ქაღალდს უნდა დაემატოს ქიმიური რეაქტივი, რათა შესაძლებელი იყოს ცვლილებების იდენტიფიცირება.

5. ქაღალდი უნდა შეიცავდეს:
   5.1. შეუიარაღებელი თვალისთვის უხილავ დამცავ ბოჭკოს, რომელიც ჩანს მხოლოდ ულტრაიისფერი სხივების ქვეშ;
   5.2. მრავალტონიან რეგისტრირებულ წყლის ნიშანს სააგენტოსთან შეთანხმებული გამოსახულებითა და ტექსტებით (მაგ., წარწერით „პასპორტი“ ინგლისურ და ქართულ ენებზე);
   5.3. გალვანოტიპის წყლის ნიშანი გვერდების ნომრების გამოსახულებით.

6. თითოეული შიდა გვერდი უნდა შეესაბამებოდეს ICAO-ს ნორმებს და უნდა შეიცავდეს, სულ მცირე, ქვემოთ ჩამოთვლილ დამცავ ელემენტებს:
   6.1. სანდო ფონი (ცისარტყელას ბეჭდვა, მიკროასოებით ბეჭდვა, გილიოშირება, ნუმიზმატური ნახატები, განზრახ დაშვებული შეცდომები);
   6.2. IR-split;
   6.3. ცისარტყელას ბეჭდვა, სულ მცირე, ორი ფერის გადასვლით (A-B-A);
   6.4. სულ მცირე, 3 (სამი) პირდაპირი ტონის შემცველი, ინფრაწითელ სპექტრში უხილავი გამოსახულება, შესრულებული ოფსეტური ბეჭდვით;
   6.5. 1 (ერთი) გამოსახულება შესრულებული უხილავი და ულტრაიისფერ სპექტრში ხილული ყვითელი მელნით;
   6.6. მიკრობეჭდვა;
   6.7. ანტისკანირების დიზაინი;
   6.8. ულტრაიისფერი დიზაინი თითოეული გვერდისთვის;
   6.9. თანმხვედრი გამოსახულება (See-through).

### 4.3.4 ბუკლეტის აკინძვა

1. ამ პუნქტის მოთხოვნები მოქმედებს #1 ცხრილში მითითებული ყველა პასპორტის ბლანკის მიმართ.

2. ბლანკი უნდა იყოს აკინძული დამცავი ძაფებით და დამცავი აკინძვის ტექნოლოგიების გამოყენებით.

3. ძაფი უნდა იყოს ფერადი და შედგებოდეს 3 (სამი) ინდივიდუალური სხვადასხვა ფერის ბოჭკოსგან, რომელიც ჩანს ულტრაიისფერი სხივის ქვეშ. გამოყენებული ძაფები უნდა

ეყრდნობოდეს მექანიზმს, რომელიც უზრუნველყოფს მათი მთლიანობის რღვევას ბუკლეტის დაშლის მცდელობის შემთხვევაში.

### 4.3.5 პასპორტის დანომვრა

1. ამ პუნქტის მოთხოვნები მოქმედებს #1 ცხრილში მითითებული ყველა პასპორტის ბლანკის მიმართ.

2. პასპორტები უნდა იყოს დანომრილი 4.8 თავის მე-8 პუნქტის მოთხოვნების შესაბამისად. პასპორტის ნომერი დატანილი უნდა იყოს ორივე ყდის შიდა გვერდზე. პასპორტის ბოლო შიდა გვერდზე პასპორტის ნომერი დამატებით დაბეჭდილი უნდა იყოს 1D შტრიხკოდის სახით. ნომერი და შტრიხკოდი უნდა დაიბეჭდოს შავი მელნით და ულტრაიისფერი სხივის ქვეშ მწვანედ უნდა ანათებდეს.

3. პასპორტი უნდა დაინომროს ბლანკის ლაზერული პერფორაციით კონუსურ ჭრილში პოლიკარბონატის მონაცემთა გვერდიდან (ჩათვლით) უკანა ყდამდე (ჩათვლით).

4. რიცხვების თანმიმდევრობა გადაეცემა მომწოდებელს ხელშეკრულების ხელმოწერის შემდეგ.

## 4.4 ზოგადი მოთხოვნები პირადობის ელექტრონული მოწმობებისა და ელექტრონული პასპორტების მონაცემთა გვერდების მიმართ

1. პირადობის ელექტრონული მოწმობისა და ელექტრონული პასპორტის მონაცემთა გვერდის გრაფიკული დიზაინი უნდა ინარჩუნებდეს მოცემული ტენდერის გამოცხადების დროისათვის მოქმედი პირადობის ელექტრონული მოწმობისა და ელექტრონული პასპორტის დიზაინის ძირითად ელემენტებს, მაგრამ ასევე უნდა შეიცავდეს ცვლილებებსაც, რაც გამყალბებლებს ხელს შეუშლის ამჟამინდელ მოდელს მიკუთვნებული მოპარული, დაკარგული და სხვა პირადობის ელექტრონული მოწმობების და ელექტრონული პასპორტების ელემენტების ხელმეორედ გამოყენებაში მაღალი ხარისხის ყალბი დოკუმენტების დამზადებისას. არსებული პირადობის ელექტრონული მოწმობის (მოქალაქის მოწმობის, დროებითი და მუდმივი ბინადრობის მოწმობის) გრაფიკული დიზაინი თან ერთვის დოკუმენტს. რაც შეეხება გრაფიკული დიზაინის დამცავ ნიშნებს, მიმწოდებელი არ არის შეზღუდული არსებული გრაფიკული დიზაინით.

2. eMRTD ნიშანი პირადობის ელექტრონულ მოწმობასა და ელექტრონული პასპორტის მონაცემთა გვერდზე დატანილ უნდა იქნეს ICAO 9303 სტანდარტის შესაბამისად.

3. შესაძლებელი უნდა იყოს პირადობის ელექტრონული მოწმობისა და ელექტრონული პასპორტის მონაცემთა გვერდზე დატანილი დოკუმენტის მფლობელის პერსონალიზებული ფოტოსურათის მარტივი ავთენტიფიკაცია და გარჩევა იმ სხვა ფოტოსურათებისგან, რომლებიც შეიძლება დამზადდეს გამყალბებლებისათვის ხელმისაწვდომი ან პოტენციურად ხელმისაწვდომი პერსონალიზაციის ტექნოლოგიების გამოყენებით (დოკუმენტის სასიცოცხლო ციკლის განმავლობაში).

4. პირველი დონის შემოწმების დროს სპეციალური მოწყობილობების გამოყენების გარეშე ადვილად შესამჩნევი უნდა იყოს პერსონალიზებული პირადობის ელექტრონული მოწმობისა და ელექტრონული პასპორტის მონაცემთა გვერდზე არსებულ, დოკუმენტის მფლობელის ფოტოსურათებზე პერსონალიზაციის აღჭურვილობის მეშვეობით განხორციელებული მანიპულაციები, დოკუმენტის ნებისმიერი ფენის მოძრობა ან შეცვლა ან გადატანა სხვა დოკუმენტზე, ან მასზე დამატება, მაგალითად, თხელი ფენის გადაკვრით, ან თავდაპირველი შემცველობის ნებისმიერი სხვა ცვლილება.

5. დოკუმენტის მფლობელის ფოტოსურათის ავტომატური ავთენტიფიკაციის მიზნით, მაგალითად, როდესაც ფოტოსურათი ამოკითხულია დოკუმენტის სკანერის საშუალებით, მომწოდებელმა სააგენტოს უნდა მიაწოდოს ორიგინალი პერსონალიზებული ფოტოს გაყალბებული ფოტოსგან გარჩევისათვის საჭირო ალგორითმი და პროგრამული უზრუნველყოფის მოდულები. სააგენტოსთვის გამჟღავნებული ალგორითმი უნდა უზრუნველყოფდეს, სულ მცირე, განსხვავების ბაზისურ დონეს პროგრამული უზრუნველყოფის მოდულებთან შედარებით, რომლებიც უფრო საფუძვლიანად ამოწმებენ დოკუმენტს. ალგორითმის სალიცენზიო სქემა საშუალებას უნდა აძლევდეს სააგენტოს, თავად შეიმუშაოს ალგორითმი და გაავრცელოს ის კომპილირებული ფორმით სააგენტოს მიერ გაცემული დოკუმენტების ავთენტიფიკაციისათვის. სააგენტოსთვის მიწოდებული პროგრამული უზრუნველყოფის მოდულები უნდა ითვალისწინებდეს მის თავისუფალ გავრცელებას სააგენტოს მიერ გაცემული დოკუმენტების ავთენტიფიკაციისათვის. ალგორითმი და პროგრამული უზრუნველყოფა უნდა გულისხმობდეს, რომ ვერიფიკატორები გამოიყენებენ საყოველთაოდ ხელმისაწვდომ სენსორულ ტექნოლოგიებს ანალიზისათვის შესაფერისი ფოტოს მისაღებად. ალგორითმი და პროგრამული უზრუნველყოფის მოდულები მიწოდებულ უნდა იქნას მოცემული ტენდერის მოთხოვნების შესაბამისად.

6. დოკუმენტზე ასევე დატანილი უნდა იყოს დოკუმენტის მფლობელის მეორეული ფოტოსურათი (ფანტომური გამოსახულება), რომელიც უნდა ჩანდეს სულ მცირე იმავე მხრიდან, საიდანაც პირველადი ფოტოსურათი ჩანს. გარდა სტანდარტული უსაფრთხო ბეჭდვის და ზედაპირული რელიეფური ელემენტებისა, ფანტომური გამოსახულება უნდა შეიცავდეს პირველი დონის, სულ მცირე, 1 (ერთი) დამცავ ნიშანს და ჩაშენებული უნდა იყოს რომელიმე ქვემოთ მოყვანილ სტრუქტურაში:

6.1. გამჭვირვალე ან ნახევრად გამჭვირვალე სტრუქტურაში;
6.2. ლინზისებრი სტრუქტურის ქვეშ სამზე მეტი რეგისტრირებული ფოტოს მეშვეობით, რომლებიც ერთად ქმნიან დოკუმენტის მფლობელის მაღალი ხარისხის ფოტოსურათს.

7. პირადობის ელექტრონული მოწმობისა და ელექტრონული პასპორტის მონაცემთა გვერდის სტრუქტურა და პერსონალიზაციის ტექნოლოგია უნდა უზრუნველყოფდეს პერსონალიზაციის პროცესის განმავლობაში ბარათისა და მონაცემთა გვერდის სხვადასხვა შრეზე ზემოქმედებას (კარბონიზებას) სხვადასხვა სიღრმით. დაუშვებელია ისეთი ტექნოლოგიების გამოყენება, რომელთა დროსაც პერსონალიზდება მხოლოდ ზედა შრე ან პერსონალიზაციის პროცესის შემდეგ მოწმობა ან მონაცემთა გვერდი იფარება ზედაპირული ფენით (ამ წესიდან გამონაკლისი დაიშვება მხოლოდ პირველადი ფოტოსურათისათვის, წინამდებარე დოკუმენტის 4.9.5.1 თავის მოთხოვნების შესაბამისად).

8. ბლანკების (ელექტრონული პირადობის მოწმობებისა და ელექტრონული პასპორტების) მონაცემთა გვერდების დამზადების პროცესში პოლიკარბონატის ფენების შეერთება (ლამინირება) ხორციელდება მხოლოდ მაღალი ტემპერატურისა და წნევის გამოყენებით (დაუშვებელია სხვა დამატებითი ასაკინძი ელემენტების გამოყენება). ტექნოლოგიურ პროცესში დასაშვებია მხოლოდ ამ მიზნისათვის შესაფერისი აღჭურვილობისა და ნედლეულის გამოყენება.

9. ელექტრონული პირადობის მოწმობისა და ელექტრონული პასპორტის მონაცემთა გვერდების სტრუქტურა უნდა უზრუნველყოფდეს დოკუმენტის გამძლეობასა და ელექტრონული კომპონენტის დაცულობას მთლიანი სავარაუდო სასიცოცხლო ციკლის განმავლობაში (10 (ათი) წელი პერსონალიზაციის დღიდან), მდგრადობას ფიზიკური და ქიმიური დეკომპოზიციისა და ყალბი დოკუმენტების დასამზადებლად ინტეგრირებული დამცავი ნიშნების განმეორებითი გამოყენების მიმართ.

10. ელექტრონული პირადობის მოწმობისა და ელექტრონული პასპორტის მონაცემთა გვერდის დამზადების პროცესში ელექტრონული პირადობის მოწმობისა და ელექტრონული პასპორტის მონაცემთა გვერდის ზედაპირში უნდა ჩაშენდეს პოზიტიური, ნეგატიური და მქრქალი რელიეფი, რომელიც შეესაბამება დამტკიცებულ დიზაინს და რამდენიმე მათგანი კვეთს ფოტოსურათის არეს.

11. პირადობის ელექტრონული მოწმობის უკანა მხარეს რელიეფური სტრუქტურით გამოსახული უნდა იყოს დოკუმენტის ნომერი, რომელიც დაიცავს დოკუმენტის მფლობელის ძირითად ფოტოსურათს და სულ მცირე ერთ ბიოგრაფიულ ინფორმაციას (სახელი ან გვარი) მოწმობის უკანა მხრიდან შეტევისგან. იგი შესრულებული უნდა იყოს იმ ზომის შრიფტით, რომ მისი დანახვა შეიძლებოდეს პირველი დონის შემოწმების დროს,.

12. დოკუმენტის სტრუქტურა უნდა იძლეოდეს პოზიტიური რელიეფის მიღების საშუალებას ლაზერული გრავირების ელემენტებისათვის. რელიეფური ლაზერული გრავირება განიხილება მოწმობის ორივე მხარისთვის და ელექტრონული პასპორტის მონაცემთა გვერდის წინა მხარისთვის.

13. ელექტრონულ პირადობის მოწმობას უნდა ჰქონდეს, მინიმუმ 3 (სამი), ხოლო ელექტრონულ პასპორტს - მინიმუმ 4 (ოთხი) ინტეგრირებული ოპტიკურად ცვლადი ელემენტი, მათ შორის:
    13.1. მინიმუმ, 1 (ერთი) დიფრაქციული ოპტიკურად ცვლადი გამოსახულების გარდამქმნელი (Diffractive optically variable image device - DOVID), რომელიც შეიცავს პირველი, მე-2 და მე-3 დონის დამცავ ნიშნებს და არ მდებარეობს მოწმობის ან მონაცემთა გვერდის ზედა ფენაზე, მაგრამ იცავს დოკუმენტის მფლობელის პირველად ფოტოსურათს;
    13.2. მინიმუმ 1 (ერთი) ელემენტი პერსონალიზებულია დოკუმენტის მფლობელის მონაცემებით;
    13.3. მინიმუმ 1 (ერთი) ელემენტი დაბეჭდილია ოპტიკურად ცვლადი მელნით (optically variable ink - OVI);
    13.4. მინიმუმ 1 (ერთი) ელემენტი დატანილია ელექტრონული პასპორტის სატიტულო გვერდზე (მონაცემთა გვერდის უკანა მხარეს), რომელიც იცავს, სულ მცირე, დოკუმენტის მფლობელის ძირითად ფოტოსურათს მოწმობის უკანა მხრიდან გაყალბებისგან.

14. ელექტრონული პირადობის მოწმობის ბლანკისა და ელექტრონული პასპორტის მონაცემთა გვერდის ფონი უნდა დაიბეჭდოს ოფსეტური ტექნოლოგიით და უნდა შეიცავდეს, მინიმუმ, შემდეგ ელემენტებს:

    14.1. პოზიტიური და ნეგატიური მრავალფერიანი გილიოში ან სხვა წვრილი ხაზები, რაც უფრო გაართულებს ორიგინალი ფოტოსურათის იმიტირებასა და რეპროდუქცირებას;
    14.2. ცისარტყელასებრი ბეჭდვა, მინიმუმ, ორი ფერით (A-B-A);
    14.3. ასლების გადაღებისა და სკანირების საწინააღმდეგო დამცავი ნიშან(ებ)ი;
    14.4. პოზიტიური და ნეგატიური მიკრო-ბეჭდვა.

15. ელექტრონული პირადობის მოწმობის და ელექტრონული პასპორტის მონაცემთა გვერდის ბლანკის ფონზე (წინა და უკანა მხარეს) დატანილი უნდა იყოს ულტრაიისფერი სპექტრში ფლუორესცენტული ნაბეჭდი, რომელიც უხილავია დღის შუქზე (და კონტრასტულია ნეიტრალური ულტრაიისფერი ნათების მიმართ). დოკუმენტზე დატანილი უნდა იყოს,

სულ მცირე, შემდეგი ელემენტები, და ერთი და იმავე კატეგორიას მიკუთვნებული ზოგიერთი ელემენტი უნდა დაიტანებოდეს ორივე გვერდზე:

15.1. მრავალფერიანი გილიოში ან/და სხვა წვრილი ხაზები, რაც უფრო გაართულებს ორიგინალი სურათის მიმსგავსებას და აღწარმოებას;

15.2. ცისარტყელასებრი ბეჭდვა;

15.3. სხვადასხვა რეაქცია ულტრაიისფერი ნათების სპექტრული პარამეტრების (ტალღის სიგრძის) ცვალებადობისას;

15.4. მაღალი გარჩევადობის უცვლადი სურათი ტრიქრომატული ულტრაიისფერი ფერების გამოყენებით.

16. ელექტრონული პირადობის მოწმობის ბლანკისა და ელექტრონული პასპორტის მონაცემთა გვერდის ფონი ასევე უნდა შეიცავდეს ელემენტებს, რომელთა შემოწმებაც შესაძლებელი იქნება ინფრაწითელი ნათებით („ინფრაწითელ ნათებაში გაუჩინარება“), რომელიც შეესაბამება ICAO-ს სტანდარტებს ოპტიკურად მანქანაკითხვადი ელემენტების გამოყენების შესახებ.

17. ელექტრონული პირადობის მოწმობის ბლანკსა და ელექტრონული პასპორტის მონაცემთა გვერდის ფონური გამოსახულების ნაბეჭდი ელემენტები ისე უნდა იყოს განაწილებული, რომ ძალიან რთული იყოს ფონური გამოსახულების დაშლა (მაგ., ობიექტის დანაწევრება პატარა კომპონენტებად) გაყალბების მიზნით და მანიპულაციები ადვილად აღმოსაჩენი იყოს.

18. დოკუმენტის ნომერი დატანილი უნდა იყოს ელექტრონული პირადობის მოწმობის ბლანკის წინა მხარეს, მისი დამზადების პროცესში.

19. პერსონალიზებული დოკუმენტის (ელექტრონული პირადობის მოწმობისა და ელექტრონული პასპორტის), მინიმუმ, ერთი ველი უნდა დამუშავდეს სააგენტოს სპეციალური (მოდიფიცირებული) ფონტით ლაზერული გრავირების საშუალებით. ფონტის დიზაინი უნდა შემუშავდეს მომწოდებლის მიერ და შეთანხმდეს სააგენტოსთან.

20. სხვა მასალების (გარდა პოლიკარბონატისა) გამოყენება დასაშვებია პასპორტის ბლანკში მონაცემთა გვერდის ჩაშენების (ჩაკერების) ადგილას (ამ დოკუმენტში მოხსენიებული, როგორც „თამასა“), იმავდროულად მთლიანობის დარღვევისაგან დაცვის მაღალი დონის უზრუნველყოფით და მასალების სხვადასხვა ფიზიკური და ქიმიური მახასიათებლების გათვალისწინებით. დაუშვებელია თამასის და მონაცემთა გვერდის შეერთება წებოს ან სხვა მწებავი მასალების გამოყენებით.

21. მონაცემთა გვერდის სტრუქტურა მდგრადი უნდა იყოს სრული ან ნაწილობრივი ფიზიკური და ქიმიური განშრევების მიმართ, რათა მანიპულაციების შემთხვევაში დარჩეს

გაყალბების ხილული ნიშნები, რომელთა აღმოჩენაც შესაძლებელი იქნება პირველი დონის შემოწმებისას.

22. მონაცემთა გვერდის, თამასის და ნაკერის დამზადებისას გათვალისწინებულ უნდა იქნეს, რომ თამასა, რომელიც ღრმად შედის მონაცემთა გვერდში ან ქმნის მონაცემთა გვერდის მთლიან ფენას და დამზადებულია სხვა მასალისგან, ამცირებს პოლიკარბონატის მონაცემთა გვერდის სტრუქტურულ ერთიანობას და დაცულობას მონაცემთა გვერდის ცალკეული ფენების გაყალბების მიზნებით განშრევების დროს. ასეთი გადაწყვეტილების შემოთავაზების შემთხვევაში, მონაცემთა გვერდის სხვადასხვა შრის შეერთება უნდა განხორციელდეს ერთსა და იმავე ლამინაციის ტემპერატურაზე მათი ერთმანეთში შედნობის გზით.

23. თამასა, მონაცემთა გვერდში მისი ჩაშენების მეთოდი და ლაზერული პერსონალიზაცია უნდა უზრუნველყოფდეს დაცულობას როგორც იმავე ან ეკვივალენტური მასალების მეშვეობით იმიტირების, ისე ორიგინალი თამასის ან სხვა დოკუმენტიდან ამოღებული თამასის გამოყენებით გაყალბებისგან. თამასის იმიტირების ან განმეორებით გამოყენების ნებისმიერი მცდელობის ამოცნობა ადვილი უნდა იყოს პირველი დონის შემოწმების დროს.

24. დოკუმენტის დამზადების პროცესში შესაძლებელი უნდა იყოს თამასაზე, მაგალითად, დოკუმენტის ნომრის დატანა.

25. თამასა უნდა შეიცავდეს პირველი ან მე-2 დონის უსაფრთხო ბეჭდვის ელემენტებს ან რელიეფურ ტვიფრს.

26. ელექტრონული პირადობის მოწმობის ბლანკი და ელექტრონული პასპორტის მონაცემთა გვერდი შეიძლება შეიცავდეს ინტეგრირებულ მე-4 დონის დამცავ ერთ ნიშანს, რომელიც კლასიფიცირდება, როგორც კონფიდენციალური. ამ დამცავი ნიშნის სპეციფიკაციისა და ჩაშენებისთვის გამოიყენება საიდუმლო ინფორმაციის დაცვის ზომები.

27. ბლანკების დიზაინის სააგენტოსთვის დასამტკიცებლად წარსადგენად მომზადებისას, მომწოდებელმა უნდა აირჩიოს მეთოდები, რომლებიც იძლევიან საბოლოო პროდუქტთან მაქსიმალურად მიახლოებულ ეფექტს.

28. სააგენტოს შეუძლია დაადასტუროს მხოლოდ ის ფერთა ტონები, რომლებიც წარმოდგენილია ორიგინალი ლამინირებული მასალით წარმოდგენილ საბოლოო პროდუქტში.

29. საბოლოო პროდუქტის დამზადება დაწყება დასაშვებია მხოლოდ სააგენტოსგან ყველა ნებართვის მიღების შემდეგ.

## 4.5 ზოგადი მოთხოვნები ჩაშენებული მიკროსქემისა და მისი პროგრამული უზრუნველყოფის მიმართ

1. ელექტრონული პირადობის მოწმობისა და ელექტრონული პასპორტის ბლანკები უნდა შეიცავდეს ჩაშენებულ პროგრამულ უზრუნველყოფას (პროგრამული უზრუნველყოფა, რომელიც მუშაობს ჩაშენებულ მიკროსქემაზე), რომელიც უზრუნველყოფილი უნდა იყოს კონტაქტური და უკონტაქტო ინტერფეისით ელექტრონული პირადობის მოწმობისათვის და უკონტაქტო ინტერფეისით ელექტრონული პასპორტისათვის.

2. მიკროსქემის მოდული და ანტენა ინტეგრირებული უნდა იყოს ბლანკში ისე, რომ მოწმობისა და მონაცემთა გვერდის ზედა ფენებში არ წარმოიქმნას ნაპრალები დოკუმენტის მთლიანი სასიცოცხლო ციკლის განმავლობაში, არ მოახდინოს გავლენა სხვა ინტეგრირებულ დამცავ ნიშნებზე და არ დაზიანდეს ოპტიკური პერსონალიზაციის პროცესში.

3. მიკროსქემის კონტაქტური ფირფიტა (ელექტრონული პირადობის მოწმობისთვის) სათანადოდ უნდა იყოს დაცული კოროზიისა და ცვეთისგან მოწმობის სასიცოცხლო ციკლის განმავლობაში (პერსონალიზაციიდან 10 (ათი) წლის განმავლობაში), მოწმობის მიზნობრივი დანიშნულებით გამოყენების შედეგად.

4. მიკროსქემა, რომლისთვისაც იქმნება ჩაშენებული პროგრამული უზრუნველყოფა სერტიფიცირებული უნდა იყოს საერთო კრიტერიუმების (Common Criteria) შესაბამისად, მინიმუმ, EAL 5+ დონეზე, BSI-CC-PP-0084-2014 ან ეკვივალენტური უსაფრთხოების პროფილის გამოყენებით.

5. მიკროსქემა აღჭურვილი უნდა იყოს უსაფრთხოების საშუალებებით არსებული და პოტენციური საფრთხეებისგან დასაცავად.

6. ელექტრონული პირადობის მოწმობის მიკროსქემას უნდა გააჩნდეს მეხსიერება (EEPROM ან FLASH), რაც უზრუნველყოფს მინიმუმ 70 კილობაიტი თავისუფალი მეხსიერების მოცულობას საჭირო აპლეტების ჩატვირთვის შემდეგ პერსონალიზაციამდე. ელექტრონული პასპორტის მიკროსქემის მეხსიერების მოცულობა საკმარისად დიდი უნდა იყოს, რომ უზრუნველყოს მონაცემთა სრული მოცულობის პერსონალიზაცია მაღალი ხარისხის ფოტოსურათით. ელექტრონული პირადობის მოწმობის მიკროსქემა უნდა იყოს A ტიპის მიკროსქემა ISO/IEC 14443 სტანდარტის შესაბამისად. თუ პირადობის

ელექტრონული მოწმობში არ არის ჩაშენებული დამხმარე მონაცემების აპლიკაცია, იგი აღჭურვილი უნდა იყოს MIFARE Classic უკონტაქტო ბარათის ემულაციის შესაძლებლობებით (სულ მცირე 1 (ერთი) კილობაიტი მეხსიერებით).

7. მიკროსქემა აღჭურვილი უნდა იყოს სიმეტრიული და ასიმეტრიული კრიპტოგრაფიული კოპროცესორებით, რომლითაც მხადაჭერილია AES, 3DES, RSA და ECC ალგორითმები.

8. მიკროსქემას უნდა შეეძლოს მონაცემთა გადაცემა 424 კბ/წმ სიჩქარით უკონტაქტო რეჟიმში.

9. **ელექტრონული პირადობის მოწმობისათვის** ჩაშენებული პროგრამული უზრუნველყოფა უნდა იყოს JavaCard ოპერაციული სისტემა (JavaCard პლატფორმა). იგი ასევე უნდა შეიცავდეს ერთ JavaCard აპლეტს, რომელიც უზრუნველყოფს შემდეგი აპლიკაციების არსებობას:
   9.1. აპლიკაცია „eMRTD აპლიკაციისათვის" საჭირო ფუნქციონალების განსახორციელებლად - ეს აპლიკაცია სავალდებულია წინამდებარე შესყიდვის ფარგლებში მოწოდებული ყველა მოწმობისათვის;
   9.2. აპლიკაცია "IAS აპლიკაციისათვის" საჭირო ფუნქციონალების განსახორციელებლად - ეს აპლიკაცია სავალდებულოა წინამდებარე შესყიდვის ფარგლებში მოწოდებული ყველა მოწმობისათვის, რომლებიც აღჭურვილია 4.6 თავის ქვეთავებით განსაზღვრული შესაძლებლობებით, გარდა 4.6.7 პუნქტისა (4.6.7 პუნქტის მხარდაჭერა სავალდებულოა იმ მოწმობებისთვის, რომლებშიც ჩაშენებული იქნება დამხმარე მონაცემების აპლიკაცია).
   9.3. აპლიკაცია „დამხმარე მონაცემების აპლიკაციისათვის" საჭირო ფუნქციონალების განსახორციელებლად - ამ აპლიკაციის მიწოდება პირობითია და მომწოდებელი უფლებამოსილია მოწმობების საწყისი კომპლექტები მიაწოდოს მის გარეშე (დაწვრილებითი ინფორმაციისათვის იხილეთ თავი 3.2).

10. **ელექტრონული პასპორტისათვის** ჩაშენებული პროგრამული უზრუნველყოფა შეიძლება იყოს JavaCard ოპერაციული სისტემა (JavaCard პლატფორმა), რომელიც აღჭურვილი იქნება ერთი JavaCard აპლეტით „eMRTD აპლიკაციისათვის" საჭირო ფუნქციონალების განსახორციელებლად ან პლატფორმისმიერი (native) აპლიკაცია „eMRTD აპლიკაციისათვის" საჭირო ფუნქციონალების განსახორციელებლად.

11. უზრუნველყოფილი უნდა იყოს ქვემოთ ჩამოთვლილი ფუნქციონალები:

    11.1. eMRTD აპლიკაციისათვის - ელექტრონული მანქანაკითხვადი სამგზავრო დოკუმენტი BAC, PACE, Chip Authentication, Terminal Authentication და Passive Authentication უსაფრთხოების მექანიზმებით დაცული ფოტოსურათითა და თითის ანაბეჭდის ბიომეტრიული მონაცემებით - კონტრაქტის მოქმედების ვადის

განმავლობაში მომწოდებელმა უნდა უზრუნველყოს შესაბამისობა უახლეს ტექნიკურ სპეციფიკაციებთან, რომლებიც საფუძვლად უდევს ევროკავშირის კანონებსა და რეგულაციებს მანქანაკითხვადი სამგზავრო დოკუმენტების შესახებ. აღნიშნული აპლიკაცია გამოიყენება როგორც ელექტრონული პირადობის მოწმობისათვის, ისე ელექტრონული პასპორტისათვისაც.

11.2. IAS აპლიკაციისათვის - კვალიფიციური ელექტრონული ხელმოწერის შექმნის მოწყობილობა, რომელიც გამოიყენება დოკუმენტის მფლობელის ელექტრონული იდენტიფიცირებისა და ავთენტიფიკაციისათვის და ელექტრონული კომუნიკაციის დაცვისათვის - კონტრაქტის მოქმედების ვადის განმავლობაში მომწოდებელმა უნდა უზრუნველყოს შესაბამისობა უახლეს ტექნიკურ სპეციფიკაციებთან, რომლებიც საფუძვლად უდევს ევროკავშირის კანონებსა და რეგულაციებს ელექტრონული იდენტიფიცირებისა და კვალიფიციური ელექტრონული ხელმოწერის შესახებ.

12. ოპერაციული სისტემა, რომელიც იყენებს JavaCard პლატფორმას (ელექტრონული პირადობის მოწმობებისა და, სურვილისამებრ, ელექტრონული პასპორტებისათვის), სერტიფიცირებული უნდა იყოს საერთო კრიტერიუმების შესაბამისად, მინიმუმ, EAL 5+ დონეზე Java Card Protection Profile – Open Configuration-ის (ან ეკვივალენტური პროფილის) გამოყენებით, რაც იძლევა საშუალებას, ელექტრონულ კომპონენტში დაინსტალირდეს დამატებითი აპლეტები მთელი სასიცოცხლო ციკლის განმავლობაში ისე, რომ არ მოახდინოს გავლენა მისი ძირითადი აპლიკაციების ფუნქციონალზე, უსაფრთხოებასა და შესაბამის სერტიფიცირებაზე.

13. მიკროსქემის ოპერაციული სისტემა უნდა აკმაყოფილებდეს, სულ მცირე, ქვემოთ ჩამოთვლილ სტანდარტებს (ეკვივალენტობა გულისხმობს სრულ ურთიერთთავსებადობას საჯაროდ ცნობილი ფუნქციონალის გამოყენების თვალსაზრისით):

13.1. Java Card 3.0.4. CE ან უფრო ახალი (ან ეკვივალენტური) ვერსია - სავალდებულოა პირადობის ელექტრონული მოწმობისათვის, არჩევითია ელექტრონული პასპორტისათვის;

13.2. Global Platform 2.2.1 ან უფრო ახალი (ან ეკვივალენტური) ვერსია;

13.3. ელექტრონული კომპონენტის ოპერაციული სისტემა უნდა უზრუნველყოფდეს SCP02 და SCP03 დაცული არხის პროტოკოლების მხარდაჭერას.

14. „დამხმარე მონაცემების აპლიკაცია“ უნდა უზრუნველყოფდეს პირადობის ელექტრონულ მოწმობაში მფლობელის მონაცემების შენახვის შესაძლებლობას კონტაქტურ და უკონტაქტო ინტერფეისზე. იგი უნდა აკმაყოფილებდეს 4.6 თავით - „დეტალური ფუნქციური მოთხოვნები IAS და დამხმარე მონაცემების აპლიკაციის მიმართ“ - განსაზღვრულ მოთხოვნებს.

15. eMRTD აპლიკაცია უნდა უზრუნველყოფდეს ECC (Brainpool-ის და NIST-ის მრუდები სავალდებულოა) და AES კრიპტოგრაფიას, ისევე როგორც SHA-2 ჰეშფუნქციის მხარდაჭერას ყველა მოქმედ უსაფრთხოების მექანიზმსა და პროტოკოლში (გარდა Active Authentication-ისა და Basic Access Control-ისა).

16. eMRTD აპლიკაციით შესაძლებელი უნდა იყოს, მინიმუმ, DG1, DG2, DG3 (DG3 დაცული უნდა იყოს დაცულია ტერმინალის ავთენტიფიკაციის მექანიზმით), DG7, DG11 და DG12 მონაცემთა ჯგუფების პერსონალიზება და ასევე იმ მონაცემთა ჯგუფების პერსონალიზება, რომლებიც დაკავშირებულია უსაფრთხოების მექანიზმების განხორციელებასთან. ხელშეკრულების გაფორმების შემდეგ სააგენტო და მომწოდებელი უნდა შეთანხმდნენ ფაილების სისტემისა და უსაფრთხოების მექანიზმების დეტალური კონფიგურაციის თაობაზე. DG3-ის პერსონალიზაცია უნდა იყოს არასავალდებულო ელექტრონული პირადობის მოწმობისათვის.

17. eMRTD აპლიკაცია უნდა უზრუნველყოფდეს დინამიკური გადაბმის (Dynamic Binding) მხარდაჭერას, მაგრამ დაუშვებელია სტატიკური უკონტაქტო იდენტიფიკატორის (UID ან PUPI) გამოყენება ელექტრონული პასპორტებისათვის.

18. მომწოდებელმა უნდა უზრუნველყოს სააგენტოსთვის ელექტრონული კომპონენტის პერსონალიზაციის გასაღების მიწოდება. პერსონალიზაციის პროცესში შესაძლებელი უნდა იყოს რომელიმე პერსონალიზაციის გასაღების შეცვლა. პერსონალიზაციის გასაღებების მიწოდება უნდა გულისხმობდეს ტრანსპორტირებას ე.წ. „გასაღებების გაცვლის გასაღების“ (KEK) მეშვეობით, რომელიც უნდა მიეწოდოს სააგენტოს 3 (სამ) სხვადასხვა გასაღების მცველს. KEK-ისა და სხვა გასაღებების მიწოდება უნდა განხორციელდეს 4.10 თავში მითითებული პროცედურის შესაბამისად.

19. IAS აპლიკაცია უნდა უზრუნველყოფდეს RSA და ECC კრიპტოგრაფიულ მხარდაჭერას შემდეგი ძირითადი ფუნქციებისთვის:

    19.1. მოწმობის მფლობელის ელექტრონული იდენტიფიცირება;
    19.2. მოწმობის მფლობელის ელექტრონული ავთენტიფიკაცია;
    19.3. კვალიფიციური ელექტრონული ხელმოწერის შექმნა;
    19.4. ელექტრონული კომუნიკაციის დაცვა (დაშიფვრა და გაშიფვრა).

20. ზემოხსენებული ძირითადი ფუნქციების შესასრულებლად საჭირო X.509 სერტიფიკატები შეიძლება გაიცეს სანდო სერვისების პროვაიდერის მიერ, რომლის სერვისებიც არ შედის წინამდებარე შესყიდვის ფარგლებში. მომწოდებელი პასუხისმგებელია მის მიერ

მისაწოდებელი კვალიფიციური ელექტრონული ხელმოწერის შექმნის მოწყობილობის შესახებ ყველა იმ საჭირო ინფორმაციის მიწოდებაზე, რაც საჭიროა სანდო სერვისების პროვაიდერის აკრედიტაციის ან რეგულარული აუდიტის პროცესისათვის.

21. აუთენტიფიკაციისა და კვალიფიციური ელექტრონული ხელმოწერის შექმნის ფუნქციები დაცული უნდა იყოს ორი სხვადასხვა PIN-ით ($PIN_{auth}$ და $PIN_{sig}$), რომლებიც დაიბლოკება PIN-ის 3-ჯერ წარუმატებლად შეყვანის შემდეგ.

22. $PIN_{auth}$ უნდა გაზიარდეს eMRTD აპლიკაციასთან და შესაძლებელი უნდა იყოს DG-ების წაკითხვა $PIN_{auth}$ -ის ავთენტიფიკაციის შემდეგ.

23. ნებადართულია პროგრამულ გადაწყვეტაში მხოლოდ ისეთი კრიპტოგრაფიული (სიმეტრიული და ასიმეტრიული) ალგორითმების, გასაღების სიგრძეების, ჰეშფუნქციებისა და მონაცემთა დაცვის სხვა მექანიზმების გამოყენება, რომლებიც იძლევიან უსაფრთხოების გარანტიას დოკუმენტის მთელი სასიცოცხლო ციკლის განმავლობაში, კომპეტენტური ორგანოების, როგორებიცაა სერტიფიცირების ორგანოები, რეკომენდაციების თანახმად.

24. ელექტრონული პირადობის მოწმობის ელექტრონული კომპონენტის კრიპტოგრაფიული ფუნქციონალები უნდა გაიტესტოს და სერტიფიცირდეს საერთო კრიტერიუმების EAL 4+ ან უფრო მაღალი სტანდარტის შესაბამისად EN 419211-ის შესაბამისი ნაწილებით განსაზღვრული დაცვის პროფილების გამოყენებით (მინიმუმ, EN 419211-2:2013, EN 419211-3:2013,EN 419211-4:2013 ან სტანდარტების ან მათში არსებული პროფილების უფრო ახალი ვერსიები).

25. პირადობის ელექტრონული მოწმობა უნდა იძლეოდეს სამომავლო განვითარების შესაძლებლობას მოწმობის მთელი სასიცოცხლო ციკლის განმავლობაში (ახალი აპლიკაციის, ახალი ფუნქციონალების ჩატვირთვა). კერძოდ, შესაძლებელი უნდა იყოს IAS აპლიკაციის სრულად დეაქტივაცია და მსგავსი ფუნქციონალობის მქონე ახალი IAS აპლიკაციის ჩატვირთვა და პერსონალიზება იმავე ფუნქციონალობით.

26. IAS აპლიკაცია უნდა აკმაყოფილებდეს 4.6 თავით - „დეტალური ფუნქციური მოთხოვნები IAS და დამხმარე მონაცემების აპლიკაციების მიმართ“ - განსაზღვრულ მოთხოვნებს.

27. კონტრაქტის გაფორმების შემდეგ მომწოდებელმა სააგენტოსთან შეთანხმებით უნდა განსაზღვროს დეტალური მოთხოვნები ელექტრონული კომპონენტის პროგრამული უზრუნველყოფის (ელექტრონული პროფილის) მიმართ. მომწოდებელმა უნდა დაიცვას ელექტრონული პასპორტისა და პირადობის ელექტრონული მოწმობის არსებული

პროფილები მაქსიმალურად, შესაძლებლობისა და გონივრულობის ფარგლებში, და განხორციელებამდე მოიპოვოს სააგენტოს დასტური.

28. სააგენტოს უნდა მიეცეს, მინიმუმ 10 (ათი) სამუშაო დღის ვადა პროგრამული უზრუნველყოფის დეტალების განსაზღვრასთან დაკავშირებით მისაწოდებელი პროდუქტების დასამტკიცებლად. საბოლოო პროდუქტის წარმოება შეიძლება დაიწყოს მხოლოდ მას შემდეგ, რაც სააგენტო დაამტკიცებს ელექტრონული კომპონენტისა და მისი პროგრამული უზრუნველყოფის სპეციფიკაციას.

29. ინტეგრირებული მიკროსქემისა და მისი პროგრამული უზრუნველყოფის ყველა ფუნქცია დოკუმენტირებული უნდა იყოს APDU დონეზე. ელექტრონული პირადობის მოწმობის ინტერფეისის აღწერილობების (სპეციფიკაციების) გამოქვეყნება სააგენტოს კომპეტენციაა და მომწოდებელს არ აქვს უფლება შეუზღუდოს სააგენტოს ამის შესაძლებლობა. ამ წესიდან გამონაკლისი შეიძლება იყოს მხოლოდ პერსონალიზაციის ბრძანებების სპეციფიკაციები, რომლებისთვისაც შეიძლება მოქმედებდეს კონფიდენციალურობის ხელშეკრულება.

30. შესაძლებელი უნდა იყოს IAS და eMRTD აპლიკაციების პერსონალიზება სრულიად უსაფრთხო რეჟიმში, სადაც ყველანაირი მოძრაობა ჩაშენებული მიკროსქემიდან ან მისკენ დაიშიფრება და დაცული იქნება MAC კოდებით.

31. თუ პირადობის ელექტრონული მოწმობით მხარდაჭერილია MIFARE-ს ოფცია, უნდა დაკმაყოფილდეს შემდეგი მოთხოვნები:
    31.1. პირადობის ელექტრონული მოწმობა ასევე უნდა უზრუნველყოფდეს აპლიკაციის პროგრამირების ინტერფეისს (API) პირადობის ელექტრონული მოწმობის ჩიპში შენახული აპლიკაციებისთვის (აპლეტებისთვის), რომლის საშუალებითაც ისინი წაიკითხავენ ან შეცვლიან MIFARE-ში შენახულ მონაცემებს.
    31.2. სააგენტოსათვის მოწმობების მიწოდებამდე უნდა განხორციელდეს MIFARE Application Directory-ის სტრუქტურის ინიციალიზება.
    31.3. MIFARE-ს უსაფრთხოების გასაღებების ინიციალიზება უნდა განხორციელდეს არასტანდარტული (non-default) მნიშვნელობებით, რაც უზრუნველყოფს გასაღებების უნიკალურობას მოწმობებისა და ასევე სექტორისათვის, გარდა 0 სექტორის A გასაღებისა (MAD გასაღები). სააგენტოს უნდა მიწოდოს უსაფრთხოების გასაღებები ან მათი შექმნის მონაცემები.

## 4.6 დეტალური ფუნქციური მოთხოვნები IAS და დამხმარე მონაცემების აპლიკაციების მიმართ

### 4.6.1 მომხმარებლის კრიპტოგრაფიული გასაღებები და სერტიფიკატები

1. კრიპტოგრაფიული გასაღების წყვილები ($PrK_{auth}$ $PuK_{auth}$) ავთენტიფიკაციისათვის და (PrKsig PuKsig) ციფრული (კვალიფიციური ელექტრონული) ხელმოწერისათვის უნდა დააგენერიროს IAS აპლიკაციამ გასაღების გენერირების მოთხოვნაზე ტერმინალის მიერ გაცემული ბრძანების პასუხად. გასაღებების თითოეული წყვილი ინდივიდუალურად უნდა იქმნებოდეს და ახლდებოდეს შეუზღუდავი რაოდენობით - იმდენჯერ, რამდენჯერაც გააგზავნის ბრძანებას ტერმინალი. გასაღების ტიპებად მხარდაჭერილი უნდა იყოს RSA-2048 და ECC-256. შესაძლებელი უნდა იყოს გასაღების ტიპის ამორჩევა, სულ მცირე, პერსონალიზაციისას. ასევე მხარდაჭერილი უნდა იყოს გასაღებების წყვილის უსაფრთხო იმპორტი.
2. PrKauth და PrKsig გასაღებები საიმედოდ უნდა იქნეს შენახული მხოლოდ ჩიპში (შემდგომში ICC), არ უნდა არსებობდეს მათი გარეთ ექსპორტის არავითარი გზა, მათ შორის, არც დაშიფრული ფორმით. შესაძლებელი უნდა იყოს თითოეული გასაღების აღნიშვნა მუდმივი მიმთითებლით (გასაღების სტატიკური იდენტიფიკატორის გამოყენებით, გასაღების იდენტიფიკატორის მოთავსებით რაიმე ფაილში, რომელსაც წინასწარ განსაზღვრული გზა ექნება, ან სხვა საშუალებებით).
3. შესაძლებელი უნდა იყოს, შესრულდეს ციფრული ხელმოწერის ოპერაცია როგორც PrKauth, ისე PrKsig გასაღების გამოყენებით. სულ მცირე, PKCS#1 v1.5 სქემა მაინც უნდა იყოს მხარდაჭერილი RSA გასაღებებისთვის. მომხმარებლის კომპიუტერზე შესაბამისი პროგრამული უზრუნველყოფის არსებობის პირობებში შესაძლებელი უნდა იყოს (PrKauth PuKauth) წყვილის გამოყენება SSL/TLS სესიებში კლიენტის ავთენტიფიკაციისათვის. ასევე, უნდა შეიძლებოდეს PrKauth-ის გამოყენებით იმ მონაცემების დეშიფრაცია, რომლებიც PuKauth-ით არის დაშიფრული.
4. როდესაც IAS აპლიკაცია პერსონალიზებულია, იმ ოპერაციებმა, რომლებშიც გამოიყენება PrKauth ან PrKsig, უნდა მოითხოვონ მომხმარებლის ავთენტიფიკაცია. კრიპტოგრაფიული ოპერაციები (ციფრული ხელმოწერა, ონლაინ ავთენტიფიკაცია, დეშიფრაცია და ა.შ.) უნდა ითხოვდნენ ავთენტიფიკაციას, შესაბამისად, PINauth და $PIN_{sig}$ კოდებით.
5. IAS აპლიკაციას უნდა შეეძლოს, სულ მცირე, ორი X509 სერტიფიკატის შენახვა ისე, რომ ერთი შეესაბამებოდეს PuKsig-ს, ხოლო მეორე - PuKauth-ს თავის ფაილების სისტემაში. შესაძლებელი უნდა იყოს თითოეული მათგანის გამოყოფა სხვა ობიექტებისგან, რომლებიც შენახულია IAS აპლიკაციის ფაილების სისტემაში.
6. IAS აპლიკაციას უნდა შეეძლოს, მინიმუმ, ორი X509 სერტიფიკატის (სერტიფიკატის გამცემი ორგანოს სერტიფიკატები) შენახვა თავის ფაილების სისტემაში. შესაძლებელი უნდა იყოს თითოეული მათგანის გამოყოფა სხვა ობიექტებისგან, რომლებიც შენახულია IAS აპლიკაციის ფაილების სისტემაში.
7. IAS აპლიკაციას უნდა შეეძლოს, მინიმუმ 2 (ორი) სხვა არააუცილებელი სერტიფიკატის შენახვა. მინიმუმ 2 (ორი) ტიპის - X509v3 PKI და X509 ატრიბუტების - სერტიფიკატი (attribute

certificate) უნდა იქნეს მხარდაჭერილი. თუ სათანადო ადგილი არის გამოუყენებელი, ამის აღმოჩენა შესაძლებელი უნდა იყოს (მაგალითად, IAS აპლიკაციაში არსებული რაიმე მეტაინფორმაციის გამოყენებით, როგორებიცაა „ფაილის ზომა ნულის ტოლია“, „ფაილი არ არსებობს“ და ა.შ.).

8. პოსტპერსონალიზაციის ფაზაში შესაძლებელი უნდა იყოს სერტიფიკატის ახლით ჩანაცვლება შეუზღუდავი რაოდენობით. წინამდებარე თავის მე-7 პუნქტით განსაზღვრული არააუცილებელი სერტიფიკატებისათვის ეს დამატებით უნდა გულისხმობდეს მანამდე გამოუყენებელ ადგილებში განლაგების შესაძლებლობას, ასევე ადგილის გამოუყენებლად მონიშვნას (სერტიფიკატის წაშლა).

9. ყველა სერტიფიკატი თავისუფლად უნდა იკითხებოდეს ICC კონტაქტური ინტერფეისიდან, უსაფრთხო სესიის და/ან მომხმარებლის ავთენტიფიკაციის აუცილებლობის გარეშე.

10. ყველა ოპერაციამ, რომელიც იყენებს ICC უკონტაქტო ინტერფეისს IASv2 პერსონალიზაციის შემდეგ, მათ შორის, სერტიფიკატის წაკითხვის ოპერაციამ, უნდა მოითხოვოს უსაფრთხო სესია.

11. მას შემდეგ, რაც მოხდება IAS აპლიკაციის პერსონალიზაცია, ისეთი ოპერაციები, როგორებიცაა სერტიფიკატის მენეჯმენტი (განთავსება და/ან ამოშლა) და გასაღების წყვილების ($PrK_{auth}$ $PuK_{auth}$ და/ან PrKsig PuKsig) გენერირება, უნდა მოითხოვდეს მომხმარებლის ავთენტიფიკაციას PINauth-ით და ტერმინალის ავთენტიფიკაციას მომხმარებლის გასაღებისა და სერტიფიკატის მართვის ტერმინალად.

12. სერტიფიკატზე ხელმოწერის მოთხოვნები (Certificate Signing Request, CSR) PuKauth-ისა და PuKsig-ისთვის დაცული უნდა იყოს შიგთავსის შეცვლისგან, როდესაც ისინი ექსპორტირდებიან IAS აპლიკაციის გარეთ. შიგთავსის შეცვლისგან დაცვის მეთოდი უნდა შეირჩეს იმგვარად, რომ გარანტირებული იყოს CSR-ის ავთენტიფიკაცია სერტიფიკატის გამცემი იმ ორგანოების მიმართ, რომლებიც პასუხისმგებელი არიან მომხმარებელთა სერტიფიკატების გაცემაზე, და იმის დადასტურება, რომ გასაღებები ნამდვილად IAS აპლიკაციით დაგენერირდა. ამისათვის გამოყენებული უნდა იყოს ჩამოთვლილთაგან ერთ-ერთი მექანიზმი:

    12.1. სერტიფიკატზე ხელმოწერის მოთხოვნები (CSR) ციფრულად უნდა იქნეს ხელმოწერილი ჩიპის ავთენტიფიკაციის გასაღების წყვილის (იხ. თავი 4.6.6 - უსაფრთხოების გაფართოებული მექანიზმები) გამოყენებით, სანამ მოხდება მათი IAS აპლიკაციის გარეთ ექსპორტი. CSR ასევე უნდა შეიცავდეს პირადობის ელექტრონული მოწმობის უნიკალურ იდენტიფიკატორს (მაგალითად, დოკუმენტის ნომერი მე-14 პუნქტის შესაბამისად);

    12.2. სერტიფიკატის მოთხოვნა შესაძლებელი უნდა იყოს მხოლოდ დაცული შეტყობინებების რეჟიმში, რომელიც მყარდება ჩიპის ავთენტიფიკაციის საშუალებით (იხ. თავი 4.6.6 - უსაფრთხოების გაფართოებული მექანიზმები), Source-MAC, Response-MAC და შიფრაციის მექანიზმების გამოყენებით.

13. IAS აპლიკაციის ფაილურ სისტემას უნდა ჰქონდეს საშუალება, იქონიოს ცალკე ელემენტარული ფაილი, რათა მასში შეინახოს, სულ მცირე, 64 (სამოცდაოთხი) ბაიტი ნებისმიერი ფორმატის მონაცემები. ფაილის შიგთავსი ჩაიწერება პერსონალიზაციისას და როგორც კი IAS აპლიკაცია პერსონალიზდება, ფაილი გახდება წაკითხვადი მხოლოდ მაშინ, როდესაც მომხმარებელი ავთენტიფიკაციას $PIN_{auth}$-ით გაივლის, და ხელმისაწვდომი, სულ მცირე, კონტაქტური ინტერფეისის მეშვეობით.

14. IAS აპლიკაციის ფაილურ სისტემას უნდა ჰქონდეს საშუალება, შეინახოს დოკუმენტის ნომერი ცალკე ელემენტარულ ფაილში. დოკუმენტის ნომერი უნდა ჩაიწეროს ან პირადობის ელექტრონული მოწმობის სააგენტოსათვის მიწოდებამდე (ამ შემთხვევაში სააგენტოს არ უნდა ჰქონდეს უფლება, შეცვალოს იგი), ან სააგენტოს უნდა ჰქონდეს უფლება, ჩაწეროს დოკუმენტის

ნომერი პერსონალიზაციისას და დაიცვას იგი არაავტორიზებული ცვლილებისაგან. დოკუმენტის ნომერი უნდა იკითხებოდეს კონტაქტური და უკონტაქტო ინტერფეისიდან (უკონტაქტო ინტერფეისიდან წაკითხვა უნდა საჭიროებდეს PACE სესიის დამყარებას 4.6.4 თავის შესაბამისად). დოკუმენტის ნომერი წაკითხვადი უნდა იყოს დაცული შეტყობინებების რეჟიმში, რომელიც ჩიპის ავთენტიფიკაციის შედეგად დამყარდება.

### 4.6.2 მომხმარებლის ავთენტიფიკაცია და პაროლების მართვა

1. ოპერაციებისთვის მომხმარებლის ავთენტიფიკაცია უნდა გულისხმობდეს IAS აპლიკაციისთვის პაროლის მიწოდებას. ყველა პაროლი უნდა იყოს სტატიკური და რიცხვითი.
2. სულ მცირე, სამი პაროლი - $PIN_{auth}$, $PIN_{sig}$ და PUK - უნდა იყოს მხარდაჭერილი.
3. დამატებით, შეიძლება მხარდაჭერილი იყოს $PIN_{transport}$ პაროლი, ან მის ნაცვლად PUK იქნეს გამოყენებული $PIN_{transport}$-ის როლში. თუ PUK არის გამოყენებული $PIN_{transport}$-ის როლში, ყველა მოთხოვნა, წაყენებული $PIN_{transport}$-ის მიმართ, გავრცელდება PUK-ზე (დამატებით თავად PUK-ის მიმართ წაყენებულ მოთხოვნებზე) და არ უნდა იქნას გაგებული ისე, რომ აუცილებელია ცალკე პაროლის სახით PINtransport-ის მხარდაჭერა.
4. $PIN_{auth}$ უნდა შედგებოდეს, მინიმუმ, 6 (ექვსი) ციფრისგან და უნდა იყოს ბლოკირებადი პაროლი.
5. $PIN_{sig}$ უნდა შედგებოდეს, მინიმუმ, 6 (ექვსი) ციფრისგან და უნდა იყოს ბლოკირებადი პაროლი.
6. PUK უნდა შედგებოდეს, მინიმუმ, 8 (რვა) ციფრისგან. ის უნდა იყოს ბლოკირებადი პაროლი და ჰქონდეს გამოყენების ზღვრული რაოდენობა. გამოყენების რაოდენობა ან უნდა იყოს წინასწარ ფიქსირებული და შეადგენდეს 10-ს (ათი), ან განისაზღვრებოდეს პერსონალიზაციის დროს და შემსყიდველს შეეძლოს, გამოყენების ლიმიტის მნიშვნელობად განსაზღვროს 10 (ათი). მას შემდეგ, რაც გამოყენების მთვლელი ნულს მიაღწევს, PUK გამოუყენებელი უნდა გახდეს - მისი გამოყენების ნებისმიერი მცდელობა უნდა სრულდებოდეს შეცდომის კოდით - „დაბლოკილია“. APDU ბრძანებების მეშვეობით შესაძლებელი უნდა იყოს წაკითხვა, რამდენჯერ იქნა გამოყენებული PUK.
7. $PIN_{transport}$ უნდა შედგებოდეს, მინიმუმ, 5 (ხუთი) ციფრისაგან და უნდა იყოს ბლოკირებადი პაროლი. მან შეიძლება გაიზიაროს PRC $PIN_{auth}$-თან ან PUK-თან.
8. ყველა ბლოკირებად პაროლს უნდა ჰქონდეს პაროლის შეყვანის მცდელობის მთვლელი (PRC), დაყენებული პერსონალიზაციის დროს ან წინასწარ განსაზღვრული ლიმიტით - 3 (სამი).
9. ბლოკირებადი პაროლის შეყვანის 1 (ერთი) არასწორი მცდელობის შემდეგ PRC შემცირდება 1-ით (ერთი).
10. იმ შემთხვევაში, როდესაც დაფიქსირდება ბლოკირებადი პაროლის სწორი ვერსია და PRC არ იქნება 0-ის (ნული) ტოლი (ან მნიშვნელობა ტოლია 1-ის (ერთი), იმ შემთხვევაში, თუ გამოყენებულია უკონტაქტო ინტერფეისი), PRC მნიშვნელობა უნდა დაუბრუნდეს საწყის ნიშნულს - 3-ს (სამი).
11. იმ შემთხვევაში, თუ PRC 1-ის (ერთი) ტოლია, IAS აპლიკაციამ აღარ უნდა მიიღოს ავთენტიფიკაციის მცდელობები უკონტაქტო ინტერფეისისგან (სულ მცირე, PACE რეჟიმში) და უპასუხოს შეცდომის კოდით - „შეჩერებული“. ამ შემთხვევაში, IAS აპლიკაციამ კვლავ უნდა მიიღოს ავთენტიფიკაციის მცდელობა კონტაქტური ინტერფეისიდან.
12. იმ შემთხვევაში, თუ PRC არის 0-ის (ნული) ტოლი, IAS აპლიკაციამ აღარ უნდა მიიღოს

ავთენტიფიკაციის მცდელობა არც კონტაქტური და არც უკონტაქტო ინტერფეისიდან და უპასუხოს შეცდომის კოდით - „დაბლოკილია“.

13. PUK შესაძლებელია გამოყენებულ იქნეს PRC-ის საწყისი ლიმიტის (3) აღსადგენად $PIN_{auth}$-ისა და $PIN_{sig}$-ისთვის, რამაც 1-ით (ერთი) უნდა შეამციროს PUK-ის გამოყენების ლიმიტი.

14. პერსონალიზაციისას მნიშვნელობები უნდა მიენიჭოს, სულ მცირე, PUK-ს და $PIN_{transport}$-ს.

15. პერსონალიზაციისას $PIN_{sig}$-ს მნიშვნელობა არ უნდა მიენიჭოს.

16. IAS აპლიკაციამ შეიძლება დართოს ნება, რომ პერსონალიზაციისას $PIN_{auth}$-ს არ მიენიჭოს მნიშვნელობა.

17. თუ რომელიმე პაროლი (სულ მცირე, $PIN_{sig}$, თუმცა შესაძლოა ასევე $PIN_{auth}$) განსაზღვრული არ არის, IAS აპლიკაციის ფუნქციონალი, რომელიც ამ პაროლით უნდა იყოს დაცული, ხელმისაწვდომი არ უნდა გახდეს მანამ, სანამ პაროლის შესაფერისი მნიშვნელობა განსაზღვრული არ იქნება. ბარათის ლეგიტიმურ მფლობელს უნდა შეეძლოს $PIN_{transport}$-ის გამოყენება ამ მნიშვნელობების განსასაზღვრად. პაროლის განსაზღვრის შემდეგ, $PIN_{transport}$ გამოუსადეგარი უნდა გახდეს მნიშვნელობის ხელახლა განსაზღვრისათვის (შენიშვნა: იმ შემთხვევაში, თუ PUK გამოიყენება $PIN_{transport}$-ის როლში, ეს შეიძლება ისევ იყოს შესაძლებელი იმ მოთხოვნების შესაბამისად, რომელსაც წინამდებარე თავი უწესებს PUK-ს).

18. თუ ტერმინალი ავთენტიფიკაციას გაივლის, როგორც „პაროლების მართვის ტერმინალი“, შესაძლებელი უნდა იყოს პერსონალიზებული IAS აპლიკაციის გადაყვანა შემდეგ მდგომარეობაში:

18.1. ყველა PRC, ასევე PUK-ის გამოყენების მთვლელი საწყის მნიშვნელობებზეა გადაყვანილი.

18.2. PUK-ს და $PIN_{transport}$-ს ახალი მნიშვნელობები აქვს მინიჭებული.

18.3. $PIN_{sig}$ გასუფთავებულია, რაც ასევე იწვევს ($PrK_{sig}$, $PuK_{sig}$) გასაღების წყვილის გასუფთავებას და შესაბამისი სერტიფიკატის წაშლას, განუყოფელი (ატომური) ოპერაციით.

18.4. $PIN_{auth}$ გასუფთავებულია, ან ახალი მნიშვნელობა აქვს მინიჭებული.

19. $PIN_{auth}$-ის ახალი მნიშვნელობის განსასაზღვრად საჭირო უნდა იყოს $PIN_{auth}$-ით ან PUK-ით ავთენტიფიკაცია. იმ შემთხვევაში, თუ PUK იქნება გამოყენებული, უნდა აღდგეს PINauth-ის მცდელობების მთვლელის საწყისი მნიშვნელობაც (3) და ასევე შემცირდეს PUK-ის გამოყენების რაოდენობა 1-ით (ერთი).

20. $PIN_{sig}$-ის ახალი მნიშვნელობის განსასაზღვრად, საჭირო უნდა იყოს $PIN_{sig}$-ით ავთენტიფიკაცია. IAS აპლიკაციამ შეიძლება დამატებით დაუშვას PUK-ის გამოყენება ახალი მნიშვნელობის განსაზღვრის მიზნით, მხოლოდ მაშინ, როცა ტერმინალი ავთენტიფიცირებულია, როგორც „პაროლების მართვის ტერმინალი“. PUK-ის გამოყენების შედეგად, უნდა აღდგეს $PIN_{auth}$-ის მცდელობების მთვლელის საწყისი მნიშვნელობაც (3) და ასევე შემცირდეს PUK-ის გამოყენების რაოდენობა 1-ით (ერთი).

21. ავთენტიფიცირებულობის მდგომარეობა $PIN_{sig}$-ის, $PIN_{transport}$-ისა და PUK-ის შემთხვევაში უნდა გაუქმდეს იმ მომდევნო ოპერაციის დასრულებისთანავე, რომელიც მოითხოვს რომელიმე შესაბამისი პაროლით ავთენტიფიკაციას. გაუქმება ნიშნავს იმას, რომ მსგავსი ბრძანების ხელმეორედ მიწოდებამ ICC-სთვის ავთენტიფიკაცია ხელახლა უნდა მოითხოვოს. მაგალითად, ავთენტიფიცირებულობის მდგომარეობა $PIN_{sig}$-ის შემთხვევაში უნდა უქმდებოდეს ციფრული ხელმოწერის ოპერაციით, რომელიც იყენებს $PrK_{sig}$-ს. თუმცა იგი არ უნდა უქმდებოდეს სერტიფიკატის წაკითხვის ბრძანებით (რადგანაც სერტიფიკატის წაკითხვას PIN კოდით

ავთენტიფიკაცია არ ესაჭიროება). მაშინაც კი, როცა გადაცემულია შედგენილი ბრძანებები (მაგ., CHANGE REFERENCE DATA APDU ძველი და ახალი მნიშვნელობებით $PIN_{sig}$-ისთვის, რაც ნიშნავს PIN-ის ავთენტიფიკაციას და PIN-ის ცვლილებას), შინაგანად უნდა აღიქმებოდეს ისე, თითქოს მეორე ბრძანებაც მოსულიყოს, და შესაბამისი პაროლის ავთენტიფიცირებულობის მდგომარეობა უნდა გაუქმდეს. ეს მდგომარეობა ასევე უნდა გაუქმდეს IAS აპლიკაციის შერჩევის შეწყვეტის (deselect) ან ICC-ის გადატვირთვის (reset) შემთხვევაში.

22. ავთენტიფიცირებულობის მდგომარეობა $PIN_{auth}$-ის შემთხვევაში შესაძლოა გაუქმდეს მისი მნიშვნელობის შეცვლისას. ეს მდგომარეობა ასევე უნდა გაუქმდეს IASv2 აპლეტის შერჩევის შეწყვეტის (deselect) ან ICC-ის გადატვირთვის (reset) შემთხვევაში.

23. ავთენტიფიცირებულობის გაუქმებისა და პაროლების ბლოკირების პრინციპები დაცული უნდა იყოს იმისდა მიუხედავად, თუ როგორაა ბრძანებები ფორმატირებული: გაერთიანებული ფორმით (მაგ., CHANGE REFERENCE DATA APDU, რომელსაც გადაეცემა ძველი და ახალი პაროლი, რაც არაცხადად ნიშნავს ჯერ ავთენტიფიკაციას და შემდეგ შეცვლას) იგზავნება, თუ ცალ-ცალკე (მაგალითად, ჯერ ცხადად იგზავნება ავთენტიფიკაციის ბრძანება და უკვე შემდეგ გადაეცემა CHANGE REFERENCE DATA APDU მხოლოდ ახალი პაროლით).

### 4.6.3 აპლეტის შერჩევა (Selection) და იდენტიფიკაცია

1. IAS აპლიკაციის ფუნქციონალი, რომელიც არ არის დაკავშირებული ძირითადი ფაილის (Master File) ფუნქციებთან (მაგ., PACE), ხელმისაწვდომი უნდა იყოს ერთი ან რამდენიმე Application Dedicated File, ADF-ის მეშვეობით, რომელთა პროგრამული შერჩევა (select) შესაძლებელი იქნება ISO/IEC 7816-ის მიხედვით.

2. IAS აპლიკაციის იდენტიფიცირებისთვის უნდა გამოიყენებოდეს აპლიკაციის იდენტიფიკატორები (Application Identifiers, AID), რომლებიც ტოლია D25000001601 (RID=D250000016, PIX=01).

3. IAS აპლიკაციის სულ მცირე, ერთი ADF-ის შერჩევისას უნდა დაბრუნდეს FCP პარამეტრები ისე, რომ მისგან შეიძლებოდეს შემდეგი ინფორმაციის მიღება: აპლიკაციის ვერსია (ძირითადი - Major, მცირე - Minor) და აპლეტის სასიცოცხლო ციკლის სტატუსი (არაპერსონალიზებული, პერსონალიზებული და ა.შ.). ძირითადი (Major) ვერსია უნდა იყოს 3 (სამი).

4. თუ დამხმარე მონაცემების აპლიკაცია გულისხმობს განცალკევებულ აპლიკაციის სპეციალურ ფაილს (ADF), დაკმაყოფილებულ უნდა იქნეს შემდეგი მოთხოვნები:

   4.1. დამხმარე მონაცემების აპლიკაციის იდენტიფიცირებისთვის უნდა გამოიყენებოდეს აპლიკაციის იდენტიფიკატორები (Application Identifiers, AID), რომლებიც ტოლია D250 00001601 (RID=D250000016, PIX=02).

   4.2. დამხმარე მონაცემების აპლიკაციის სულ მცირე, ერთი ADF-ის შერჩევისას უნდა დაბრუნდეს FCP პარამეტრები ისე, რომ მისგან შეიძლებოდეს შემდეგი ინფორმაციის მიღება: აპლიკაციის ვერსია (ძირითადი - Major, მცირე - Minor) და აპლეტის სასიცოცხლო ციკლის სტატუსი (არაპერსონალიზებული, პერსონალიზებული და ა.შ.).

### 4.6.4 დაცული სესიები და დამხმარე გასაღებები

1. IAS აპლიკაციას უნდა შეეძლოს, დაამყაროს დაცული სესიები და მოითხოვოს აღნიშნული სესიები უსაფრთხოების თვალსაზრისით კრიტიკული ოპერაციებისთვის.
2. ყველა უსაფრთხო სესია უნდა ემყარებოდეს ფორმას: დაშიფვრა-შემდგომ-ავთენტიფიკაცია. სულ მცირე, ტერმინალიდან აპლეტისთვის გადაცემული მოთხოვნები უნდა იყოს დაცული ამ მეთოდით.
3. IAS აპლიკაციის პერსონალიზაციის შემდეგ, უკონტაქტო ინტერფეისით მასზე მიმართვამ უნდა მოითხოვოს დაცული სესიის დამყარება პაროლზე დაფუძნებული ავთენტიფიკაციით (PACE პროტოკოლი) ნებისმიერი ოპერაციის წინ.
4. PACE პროტოკოლი რეალიზებული უნდა იყოს მანქანაკითხვად სამგზავრო დოკუმენტებზე ICAO-ს მოთხოვნების (ICAO Doc 9303) მიხედვით.
5. PACE ფუნქციონირება მხარს უნდა უჭერდეს, სულ მცირე, PINauth და, ასევე, CAN და MRZ პაროლებს, მაგრამ MRZ-სა და CAN-ზე დაფუძნებული ავთენტიფიკაცია რეზერვირებული უნდა იყოს ბარათის სხვა აპლეტებისათვის, მაგალითად, eMRTD აპლიკაციისთვის. CAN და MRZ-ავთენტიფიცირებული სესია უნდა განიხილებოდეს, როგორც არაავთენტიფიცირებული IAS აპლიკაციის ფუნქციონალობისთვის.
6. შესაბამისი პაროლით და PACE ავთენტიფიკაციის შემდგომ, უნდა შეიძლებოდეს ისეთი ოპერაციის შესრულება, რომელიც მოითხოვს მომხმარებლის ავთენტიფიკაციას შესაბამისი პაროლით. ეს ფუნქცია ხელმისაწვდომი უნდა იყოს PINauth-ისთვის.
7. კონტაქტურმა ინტერფეისმა უნდა დაუშვას ორივე, დაცული (PACE-ით) და დაუცველი წვდომა.
8. PACE ავთენტიფიკაცია ხელმისაწვდომი უნდა იყოს, როგორც ბარათის გლობალური სერვისი, რაც ნიშნავს, რომ მისი გამოყენება უნდა შეეძლოთ ICC-ზე მოთავსებულ სხვა აპლეტებს (eMRTD და დამხმარე მონაცემების აპლიკაციებს). კერძოდ, იგივე PACE-ის შესაძლებლობის გამოყენება შესაძლებელი უნდა იყოს eMRTD აპლიკაციისათვის, რათა მოხდეს წვდომის დამატებითი კონტროლის (Supplemental Access Control) მხარდაჭერა. აღნიშნული უნდა შეიძლებოდეს PINauth-ით და MRZ-ით, მაგრამ არ უნდა შეიძლებოდეს PUK, $PIN_{sig}$ და $PIN_{transport}$-ით. მეტიც, აღნიშნული „გლობალური სერვისის“ შესაძლო კომპრომეტირება (მაგ., პოსტპერსონალიზაციის გასაღებების კომპრომეტირება, რომელმაც შეიძლება მისცეს უფლება, რომ ჩაიტვირთოს მავნე აპლეტები ან ჩანაცვლდეს ლეგიტიმური აპლეტებიც კი) არ უნდა ქმნიდეს (PrKsig, PuKsig) გასაღების წყვილით კრიპტოგრაფიული ოპერაციის შესრულების რისკს ბოროტმოქმედის მიერ.
9. უსაფრთხო სესიის დამყარების შემდეგ ავთენტიფიკაცია ყველა სხვა პაროლის მეშვეობით უნდა შეიძლებოდეს VERIFY APDU ბრძანებისა და ღია ტექსტით მიწოდებული პაროლის გამოყენებით.
10. კონტაქტური ინტერფეისი უნდა უშვებდეს როგორც PACE-ავთენტიფიცირებულ უსაფრთხო სესიებს, ისე მარტივ, არაავთენტიფიცირებულ სესიებს. ამ უკანასკნელ შემთხვევაში, პაროლით ყველა ავთენტიფიკაცია უნდა ხდებოდეს VERIFY APDU ბრძანებისა და ღია ტესტით მიწოდებული პაროლის მეშვეობით.
11. ყველა ეფემერულ გასაღებს (Ephemeral Key) უნდა ჰქონდეს ICC პლატფორმის მიერ მხარდაჭერილი მაქსიმალური უსაფრთხოება.

### 4.6.5 თავსებადობა „ჭკვიანი ბარათების“ (Smart Cards) წამკითხველებთან

1. ყველა ფუნქციონალი რომელიც განსაზღვრულია საბოლოო მომხმარებლის პერსონალურ კომპიუტერზე „ჭკვიანი ბარათით” სამუშაოდ (მოცემული ტენდერით გათვალისწინებული მიდლვეარით ან მის გარეშე) დაუცველ რეჟიმში (ანუ დაცული შეტყობინებებით კომუნიკაციის გამოუყენებლად), უნდა იყოს ხელმისაწვდომი სტანდარტული სიგრძის APDU ბრძანებებითა და პასუხებით. დასაშვებია პარალელურად გაფართოებული სიგრძის APDU ბრძანებებისა და პასუხების გამოყენება. პერსონალიზაციის ბრძანებებისთვის და უსაფრთხოებასთან დაკავშირებული ბრძანებებისთვის მსგავსი ლიმიტი არ არის დაწესებული.
2. Plaintext Offline PIN ანუ ღია ტექსტური ოფლაინ PIN ბრძანებები (შემოწმება და მენეჯმენტი) უნდა იქნეს მხარდაჭერილი კონტაქტურ ინტერფეისზე PINauth, $PIN_{sig}$, $PIN_{transport}$ და PUK-ისთვის.

### 4.6.6 უსაფრთხოების გაფართოებული მექანიზმები

1. IAS აპლიკაცია მხარს უნდა უჭერდეს ჩიპისა და ტერმინალის ავთენტიფიკაციას. აღნიშნული პროტოკოლები და მათი ვერსიები უნდა შეესაბამებოდეს ICAO Doc 9303-ის მიერ დაშვებულ შესაბამის პროტოკოლებსა და ვერსიებს.
2. სულ მცირე, 256-ბიტიანი Elliptic Curve (EC) გასაღებები და BrainpoolP256r1 მრუდი უნდა იქნეს მხარდაჭერილი.
3. IAS აპლიკაციას უნდა ჰქონდეს საშუალება, დაადასტუროს ჩიპის ნამდვილობა, eMRTD აპლიკაციის ჩართულობის გარეშე (DG14 ფაილის და დოკუმენტის ხელმომწერის ციფრული ხელმოწერის გამოყენება) - მაგალითად, ჩიპის ავთენტიფიკაციის გასაღების პასიურ ავთენტიფიკაციაზე დაყრდნობით სერტიფიკატის გამცემი სპეციალური ორგანოს გამოყენებით.
4. ჩიპის ავთენტიფიკაციის ღია გასაღები არ უნდა იყოს ICC-დან წაკითხვადი მომხმარებლის ავთენტიფიკაციის გარეშე (თავი 4.6.2-ის შესაბამისად - მომხმარებლის ავთენტიფიკაცია და პაროლების მართვა) - სულ მცირე, უკონტაქტო ინტერფეისიდან.
5. პრივილეგირებული ტერმინალების, სულ მცირე, შემდეგი უფლებები უნდა იყოს მხარდაჭერილი ტერმინალის ავთენტიფიკაციისას:
    5.1. სერტიფიკატის მართვის ტერმინალი;
    5.2. პაროლის მართვის ტერმინალი.
6. IAS აპლიკაციას უნდა შეეძლოს მონაცემების შენახვა 2 (ორი) CVCA-სთვის, რაც საკმარისია ტერმინალური ავთენტიფიკაციის განსახორციელებლად. სულ მცირე, ერთი CVCA მონაცემები ჩაიწერება პერსონალიზაციის დროს. დამატებით, დაკმაყოფილებული უნდა იყოს შემდეგი მოთხოვნები:

    6.1. შესაძლებელი უნდა იყოს სერტიფიკატების გაცემა პრივილეგირებული ტერმინალებისათვის სერტიფიკატების გამცემი ორგანოთი, რომელიც განსხვავდება DVCA-ებისგან (სერტიფიკატების გამცემი ორგანოები, რომლებიც სერტიფიცირებულია იმავე CVCA-ს მიერ, რათა გასცენ შემოწმების სისტემის სერტიფიკატები eMRTD აპლიკაციაში წვდომის მიზნით) და უზრუნველყოფილი იყოს, რომ DVCA-ს მიერ გაცემული სერტიფიკატები არ

იქნება განხილული, როგორც პრივილეგირებული ტერმინალები;

6.2. შესაძლებელი უნდა იყოს, რომ პრივილეგირებული ტერმინალებისთვის გამოყენებულ იქნეს CVCA კავშირის სერტიფიკატები CVCA მითითებების განახლების მიზნით და ეს შესაძლებლობა არ უნდა უშლიდეს ხელს ინსპექტირების სისტემებს (სისტემებს, რომლებიც მუშაობენ DVCA-ს მიერ გაცემული სერტიფიკატებით), გამოიყენონ CVCA კავშირის სერტიფიკატები იმავე მიზნებისათვის;

6.3. თუ IAS აპლიკაცია და eMRTD აპლიკაცია იზიარებენ ერთსა და იმავე CVCA მონაცემებს, ეს არ გულისხმობს იმას, რომ CVCA კავშირის სერტიფიკატები, რომლებიც მიწოდებულია ინსპექტირების სისტემებისა და პრივილეგირებული ტერმინალებისათვის, შეიცავენ ერთსა და იმავე მონაცემებს ყველა ველსა და გაფართოებაში (ცხადია, ველების, როგორიცაა სერტიფიკატის გამცემი ორგანო, ღია გასაღები, სერტიფიკატის მფლობელი, მოქმედების ვადა იქნება იგივე).

7. იმისათვის, რათა მოხდეს ტერმინალის ავთენტიფიკაცია პრივილეგირებულ ტერმინალად, როგორიცაა სერტიფიკატის მართვის ტერმინალი ან პაროლის მართვის ტერმინალი, ჯერ უნდა მოხდეს ჩიპის ავთენტიფიკაცია, რასაც მოჰყვება გადართვა დაცულ სესიაში ENC, S_MAC და R_MAC მექანიზმების გააქტიურებით და ტერმინალის ავთენტიფიკაცია შესაბამისი უფლებამოსილებით.
8. IAS აპლიკაციას უნდა შეეძლოს იმუშაოს ჩვეულებრივ, „არაპრივილეგირებულ“ რეჟიმში ჩიპის წარმატებული ავთენტიფიკაციისა და შესაბამის დაცულ სესიაში გადართვის შემდეგ, თუკი არ ყოფილა ტერმინალის ავთენტიფიკაციის მცდელობა (მაგ., ამ რეჟიმში დაშვებული უნდა იყოს კრიპტოგრაფიული ოპერაციები ($PrK_{auth}$, $PuK_{auth}$) ან ($PrK_{sig}$, $PuK_{sig}$) გასაღების წყვილებით - წინამდებარე დოკუმენტით განსაზღვრული წინაპირობების გათვალისწინებით).
9. ტერმინალის შესაბამისი სერტიფიკატით ავთენტიფიკაციის შემდეგ, სერტიფიკატის მართვის ტერმინალს და პაროლის მართვის ტერმინალს არ უნდა შეეძლოს კრიპტოგრაფიული ოპერაციის განხორციელება ($PrK_{sig}$, $PuK_{sig}$) გასაღების წყვილით.
10. თუ ტერმინალი ავთენტიფიკაციას გაივლის, როგორც პრივილეგირებული ტერმინალი, ICC-ს გადაყვანა უკან „ნორმალურ“ (არაპრივილეგირებულ) რეჟიმში სამუშაოს დასრულების შემდეგ არ უნდა მოითხოვდეს ICC-ს გადატვირთვას (არც „თბილი“, არც „ცივი“ გადატვირთვით).

### 4.6.7 მოთხოვნები Single Sign On შესაძლებლობის მიმართ

1. IAS აპლიკაცია მესამე მხარის აპლიკაციებს უნდა უზრუნველყოფდეს Single Sign On შესაძლებლობით, რომელიც შესაძლოა მოგვიანებით განთავსდეს პირადობის ელექტრონული მოწმობის ჩიპზე სააგენტოს მიერ. კერძოდ, ის საშუალებას უნდა აძლევდეს JavaCard პაკეტებში არსებულ სხვა აპლიკაციებს, რომ საკუთარი საჭიროებებისთვის გამოიყენონ IAS აპლიკაციის ფუნქციონალები javacard.framework.Shareable ან მსგავსი მექანიზმებით, რომელიც იძლევა აპლეტებს შორის კომუნიკაციის საშუალებას აპლეტის ფაირვოლის (applet firewall) გავლით.
2. გაზიარებულ უნდა იქნას შემდეგი შესაძლებლობები:

2.1. PACE-ი $PIN_{auth}$-ის და CAN -ის გამოყენებით (სხვა პაროლების მხარდაჭერა არ არის აუცილებელი);

2.2. Plaintext $PIN_{auth}$-ის ვერიფიკაცია;

2.3. ჩიპის ავთენტიფიკაცია, მათ შორის ჩიპის ავთენტიფიკაციის გასაღებების ავთენტურობის უზრუნველყოფა;

2.4. ტერმინალის ავთენტიფიკაცია;

2.5. IAS აპლიკაციაში ჩაწერილი დოკუმენტის ნომრის წაკითხვა.

3. PACE-ის შესაძლებლობების გაზიარება შეიძლება შემოიფარგლოს შემდეგნაირად:

3.1. არ არის სავალდებულო, სხვა აპლეტებს მიეცეს საშუალება გამოიყენონ PACE არხი, რომელიც დამყარებულია MF-ით (Master File) და მისაღებია MF-ისგან განსხვავებული ფაილით დაცული არხის დამყარების მოთხოვნა (მაგ. აპლიკაციის სპეციალური ADF-ით). თუმცა, PACE დომეინის პარამეტრები და სხვა საჯაროდ წაკითხვადი PACE-სთან დაკავშირებული მონაცემები უნდა დარჩეს ჩაწერილი MF-ში;

3.2. $PIN_{auth}$-ის შეყვანის მთვლელის მაჩვენებლის შემცირება ვალიდაციის წარუმატებლობის შემთხვევაში და $PIN_{auth}$-ის დაბლოკვა თუ მთვლელის მაჩვენებელი მიაღწევს 0-ს (ნული).

4. Plaintext $PIN_{auth}$-ის ვერიფიკაციის შესაძლებლობის გაზიარება შეიძლება შემოიფარგლოს PIN-ის მნიშვნელობის შემოწმებით (რაც ასევე მოიცავს $PIN_{auth}$-ის შეყვანის მთვლელის მაჩვენებლის შემცირებას ვალიდაციის წარუმატებლობის შემთხვევაში და $PIN_{auth}$-ის დაბლოკვას თუ მთვლელის მაჩვენებელი მიაღწევს 0-ს (ნული)).

5. დასაშვებია, ჩიპის ავთენტიფიკაციის მექანიზმის გაზიარება გულისხმობდეს რომ APDU ბრძანებები ტერმინალიდან გაეგზავნება არა MF-ს (Master File), არამედ სხვა ფაილს (მაგ. IAS-ისგან განსხვავებული აპლიკაციის სპეციალურ ADF-ს) და მასთან დამყარდება დაცული არხი.

6. ტერმინალის ავთენტიფიკაციის გაზიარება შეიძლება შემოიფარგლოს ტერმინალის სერტიფიკატების CVCA-სთან ვალიდირებით, CVCA მითითებების განახლებით, თუ წარმოდგენილი იყო კავშირის სერტიფიკატი.

7. ამ შესაძლებლობის განხორციელებისას, IAS აპლიკაციამ არასდროს არ უნდა დაუბრუნოს Plaintext $PIN_{auth}$ -ი სხვა აპლიკაციებს.

8. IAS აპლიკაციისთვის ნებადართულია, რომ ყველა APDU ბრძანება ტერმინალზე დამუშავდება მესამე მხარის აპლიკაციის მიერ. თუმცა, ასევე შესაძლებელია APDu ბრძანებაზე დაფუძნებული გაცვლა მესამე მხარის აპლიკაციასთან იმის გათვალისწინებით, რომ მესამე მხარის აპლიკაციას შესაძლებლობა ექნება აკონტროლოს IAS აპლიკაციიდან დაბრუნებული საპასუხო APDU-ების სტატუსები.

9. მომწოდებელმა სააგენტოს უნდა მიაწოდოს აპლიკაციის ნიმუში კომპილირებული და საწყისი კოდის ფორმით, რომლითაც ნაჩვენები იქნება ყველა გაზიარებული შესაძლებლობის გამოყენების მაგალითები. მიწოდება უნდა განხორციელდეს არაუგვიანეს იმ პირადობის ელექტრონული მოწმობების მოწოდებისა, რომლებიც Single Sign On შესაძლებლობით იქნებიან აღჭურვილი.

### 4.6.8 მოთხოვნები დამხმარე მონაცემების აპლიკაციის მიმართ

1. დამხმარე მონაცემების აპლიკაცია საშუალებას უნდა აძლევდეს სააგენტოს შეინახოს დამატებითი ინფორმაცია ბარათის მფლობელის შესახებ პირადობის ელექტრონულ მოწმობაში მფლობელის თანხმობის საფუძველზე. ინფორმაცია შეიძლება იყოს სტუდენტის სტატუსი, ფასდაკლების ბარათის შესახებ ინფორმაცია, და სხვ. დამხმარე მონაცემების აპლიკაცია უნდა უზრუნველყოფდეს მომხმარებლის ავთენტიფიკაციის მხარდაჭერას $PIN_{auth}$-ით, რომელიც იქნება იგივე და იმართება IAS აპლიკაციის მიერ. $PIN_{auth}$-ით ავთენტიფიკაცია უკონტაქტო ინტერფეისზე მოითხოვს PACE პროტოკოლს.
2. დამხმარე მონაცემების აპლიკაციაში წვდომა შესაძლებელია განხორციელდეს კონტაქტური ან უკონტაქტო ინტერფეისის საშუალებით. თუ მკაფიოდ არ იქნება განსაზღვრული, წინამდებარე თავში მოყვანილი ყველა მოთხოვნა შეეხება ორივე ინტერფეისს.
3. დამხმარე მონაცემების აპლიაციას უნდა შეეძლოს შეინახოს ნებისმიერი მონაცემი ელემენტარულ ფაილებში (EF).
4. EF-ებზე ყველა კონტენტთან დაკავშირებული ოპერაციის განხორციელება შესაძლებელი უნდა იყოს APDU ბრძანებების გამოყენებით ISO/IEC 7816-ის მე-4 ნაწილის შესაბამისად. კერძოდ:
    4.1. ფაილის არჩევა - SELECT APDU;
    4.2. ფაილის კონტენტის მართვა - UPDATE BINARY (არააუცილებელი - WRITE BINARY, ERASE BINARY);
    4.3. ფაილის კონტენტის წაკითხვა - READ BINARY.
5. დამხმარე მონაცემების აპლიკაცია უნდა უზრუნველყოფდეს ერთდრულად სულ მცირე 32 (ოცდათორმეტი) EF-ის მხარდაჭერას. თუ სააგენტოსთვის შეუძლებელია საჭიროებიდან გამომდინარე მეტი EF-ის დინამიკურად შექმნა, სააგენტოს უნდა შეეძლოს მოსთხოვოს მომწოდებელს გაზარდოს ეს რაოდენობა პირადობის ელექტრონულ მოწმობებთან დაკავშირებით მისაწოდებელი მასალების შემდეგი პარტიისათვის წინამდებარე შესყიდვის ფარგლებში - პირადობის ელექტრონული მოწმობების ჩიპის მოდულების შეზღუდვების გათვალისწინებით.
6. სააგენტო უფლებამოსილი უნდა იყოს, მიანიჭოს EF-ს იდენტიფიკატორი სულ მცირე 2 (ორი) ბაიტის შემცველობით, ან გააუქმოს აღნიშნული იდენტიფიკატორის მინიჭება. დამხმარე მონაცემების აპლიკაცია უნდა უზრუნველყოფდეს EF-ის არჩევას ამ იდენტიფიკატორის მეშვეობით SELECT APDU ბრძანებით ISO/IEC 7816-ის მე-4 ნაწილის შესაბამისად. მხოლოდ სააგენტოს უნდა შეეძლოს ერთპიროვნულად გადაწყვიტოს რა მნიშვნელობის იდენტიფიკატორს გამოიყენებს მინიჭების დროს. მომწოდებლის შეხედულებისამებრ, ფაილის იდენტიფიკატორის მინიჭება შეიძლება გულისხმობდეს ფაილის შექმნას, ხოლო მინიჭების გაუქმება შეიძლება გულისხმობდეს ფაილის წაშლას.
7. სააგენტოს შესაძლებლობა უნდა ჰქონდეს, რომ რომელიმე EF გახადოს, სურვილისამებრ, და ოპერაციათა რაოდენობის შეუზღუდავად:
    7.1. საჯაროდ წაკითხვადი - არ არის საჭირო მომხმარებლისგან რაიმე ქმედების (მაგ. PACE არხის დამყარება, $PIN_{auth}$-ით ავთენტიფიკაცია) განხორციელება, ტერმინალს ყოველთვის შეუძლია მისი წაკითხვა;
    7.2. წაკითხვადი ავთენტიფიცირებული სესიების საშუალებით (როდესაც მომხმარებლის

ავთენტიფიკაცია ხორციელდება $PIN_{auth}$-ით);

7.3. წაკითხვადი PACE -ს საშუალებით (სულ მცირე როდესაც PACE დამყარებულია CAN-ის ან $PIN_{auth}$-ის გამოყენებით);

7.4. წვდომის სხვა პირობების მხარდაჭერა არ არის სავალდებულო.

8. თუ EF არ არის საჯაროდ წაკითხვადი, უკონტაქტო ინტერფეისისთვის შესაძლებელი უნდა იყოს მისი წაკითხვა მხოლოდ იმ შემთხვევაში თუ დამყარებულია PACE არხი.

9. თუ EF არის საჯაროდ წაკითხვადი, დამხმარე მონაცემების აპლიკაცია მაინც შეიძლება ეყრდნობოდეს კრიპტოგრაფიულ ოპერაციებს (როგორიცაა სიმეტრიული გასაღებები გასაღებების დივერსიფიკაციის მხარდაჭერით ან მის გარეშე), მაგრამ არც სააგენტოს და არც მესამე მხარეს, ვისაც სურს ასეთი ფაილების წაკითხვა, არ უნდა დაუწესდეს შეზღუდვები, მაგ. სპეციალური აპარატურის შესყიდვა, სალიცენზიო მოსაკრებლის გადახდა და ა.შ.

10. ჩიპის ავთენტიფიკაციის პროტოკოლი მხარდაჭრილი უნდა იყოს დამხმარე მონაცემების აპლიკაციის მიერ. თუ EF არ არის საჯაროდ წაკითხვადი, შესაძლებელი უნდა იყოს მისგან მონაცემების წაკითხვა დაცულ არხში, რომელიც დამყარდება ჩიპის ავთენტიფიკაციის პროტოკოლით, იმის გათვალისწინებით, რომ ასევე დაკმაყოფილებულია მასზე წვდომის პირობები მე-5 პუნქტის თანახმად. შესაძლებელი უნდა იყოს მოწმობის ჩიპის ავთენტიფიკაციის გასაღებების ავთენტიფიკაცია.

11. არ არის აუცილებელი EF-ებში კონტაქტური და უკონტაქტო ინტერფეისებიდან წვდომის სხვადასხვა პირობების მხარდაჭერა.

12. ფაილის შიგთავსის მართვის ოპერაციები (პუნქტი 4.2.), ისევე როგორც ფაილის იდენტიფიკატორის მინიჭებისა და გაუქმების ოპერაციები (პუნქტი 6) და ფაილზე უსაფრთხოების ატრიბუტების დაყენების ოპერაციები (პუნქტი 7) შესაძლებელი უნდა იყოს მხოლოდ იმ შემთხვევაში, თუ მოწმობის მფლობელი გაივლის ავთენტიფიცირებას და მოქმედებს პრივილეგირებული ტერმინალი. კერძოდ:

12.1. მომხმარებელმა უნდა გაიაროს ავტენტიფიკაცია $PIN_{auth}$-ით;

12.2. უნდა დამყარდეს ჩიპის ავთენტიფიკაციის სესია;

12.3. ტერმინალის ავთენტიფიკაცია უნდა განხორციელდეს 4.6.6. თავის თანახმად (უსაფრთხოების გაფართოებული მექანიზმები). ტერმინალის ავთენტიფიკაციისათვის დაუშვებელია პაროლის მართვის ტერმინალის უფლებების მოთხოვნა, თუმცა შესაძლებელია გამოყენებულ იქნას სერტიფიკატის მართვის ტერმინალის უფლებები ან დანერგილ იქნას ახალი ტიპის პრივილეგირებული ტერმინალი.

12.4. სხვა უსაფრთხოების მექანიზმები არ არის სავალდებულო.

13. დასაშვებია, დამხმარე მონაცემების აპლიკაცია განცალკევებული იყოს IAS აპლიკაციისგან და უნდა იყენებდეს IAS აპლიკაციის Single Sign On შესაძლებლობას (თავი 4.6.7.) როდესაც მოთხოვნილია $PIN_{auth}$-ი, CAN, ჩიპის ავთენტიფიკაცია ან ტერმინალის ავთენტიფიკაცია.

## 4.7 მოთხოვნები შუალედური პროგრამული უზრუნველყოფის მიმართ

1. შუალედური პროგრამული უზრუნველყოფა უნდა უზრუნველყოფდეს იმას, რომ IAS აპლიკაციის ფუნქციონალები ხელმისაწვდომი იყოს დამოკიდებული აპლიკაციებისათვის მიზნობრივ ოპერაციულ სისტემებსა და გამომთვლელ მოწყობილობებზე სტანდარტული ინტერფეისების გამოყენებით. შუალედური პროგრამული უზრუნველყოფა უნდა შემუშავდეს ღია სტანდარტებისა და დოკუმენტაციის გამოყენებით, გააძლიეროს სააგენტოს ამჟამინდელი შუალედური პროგრამული უზრუნველყოფა და უზრუნველყოს სრული მხარდაჭერა უკვე გაცემული ელექტრონული პირადობის მოწმობებისათვის.

2. კონტრაქტის გაფორმების შემდეგ სააგენტო უზრუნველყოფს მომწოდებელს წვდომით შუალედური პროგრამული უზრუნველყოფის არსებულ საწყის კოდზე, რომელიც ეფუძნება OpenSC ბიბლიოთეკას და დოკუმენტაციაზე. საწყის კოდზე წვდომის მინიჭება მოხდება სააგენტოს Git რეპოზიტორიაზე. მომწოდებლის მიერ მიწოდებულ შუალედური პროგრამული უზრუნველყოფასთან დაკავშირებულ მასალებს უნდა მიენიჭოს ვერსიის ნომრები, და იმავე ვერსიის სტრინგები უნდა მიეთითოს გიტ-რეპოზიტორიაში (მაგ. შესაბამისი თეგების მითითებით).

3. მომწოდებელმა უნდა უზრუნველყოს შუალედური პროგრამული უზრუნველყოფის საწყისი კოდის შემდგომი მართვა სააგენტოს მიერ განსაზღვრულ პლატფორმაზე, მისცეს სააგენტოს თავისუფალი წვდომა საწყის კოდზე და საშუალება, განსაზღვროს კოდის გამოქვეყნების საკუთარი პოლიტიკა.

4. შუალედური პროგრამული უზრუნველყოფის ლიცენზიის პირობები განისაზღვრება სააგენტოს მიერ და მომწოდებელს უფლება არ აქვს, დაიტოვოს ინტელექტუალური საკუთრების უფლებები შუალედურ პროგრამულ უზრუნველყოფასთან დაკავშირებით.

5. მომწოდებელმა უნდა უზრუნველყოს შუალედური პროგრამული უზრუნველყოფის დროული მხარდაჭერა Microsoft Windows 7, 8.1,10 და შემდგომი ვერსიების, Apple (macOS) 10.9 და შემდგომი ვერსიების და Linux-ის (Ubuntu linux 12.04 და ზემოთ, შეიძლება შეიზღუდოს მხოლოდ LTS-მდე) ოპერაციული სისტემების უახლესი ვერსიებისათვის კონტაქტის მოქმედების ვადის განმავლობაში "ჭკვიანი ბარათისა" და კრიპტოგრაფიული ობიექტის დამუშავების მეთოდებით, როგორიცაა CNG, MS CAPI (MS CAPI შეიძლება მხარდაჭერილი იყოს CNG-ს მეშვეობით), Minidriver, CryptoTokenKit, რომლებიც შეესაბამება თითოეულ ოპერაციულ სისტემას. PKCS#11 მხარდაჭერილი უნდა იყოს ყველა პლატფორმისთვის.

6. შუალედური პროგრამული უზრუნველყოფა უნდა უზრუნველყოფდეს ქვემოთ მოყვანილ მინიმალურ ფუნქციონალებს:

6.1. მოწმობის მფლობელის ელექტრონული იდენტიფიცირება - მონაცემების მოპოვება (წაკითხვა) ელექტრონული პირადობის მოწმობის ელექრონული კომპონენტის „ელექტრონული პირადობის მოწმობის „IAS აპლიკაციის მონაცემთა ჯგუფიდან ან/და სერტიფიკატიდან, მათ შორის, შესაბამისი სერტიფიკატების წაკითხვა, ცალმხრივი და ორმხრივი ავთენტიფიკაციის განხორციელების შესაძლებლობით.

6.2. მოწმობის მფლობელის ელექტრონული ავთენტიფიკაცია ავთენტიფიკაციის სერტიფიკატისა და შესაბამისი ავთენტიფიკაციის დახურული გასაღების მეშვეობით, რა შემთხვევაშიც მოწმობის მფლობელს მოეთხოვება, შეიყვანოს საიდუმლო $PIN_{auth}$.

6.3. კვალიფიციური ელექტრონული ხელმოწერის შექმნა ხელმოსაწერი მონაცემების ან შესაბამისი ჰეშმნიშვნელობის, მოწმობის მფლობელის კვალიფიციური სერტიფიკატის და ელექტრონული ხელმოწერის შესაბამისი დახურული გასაღების (ელექტრონული ხელმოწერის შექმნისთვის საჭირო მონაცემების) გამოყენებით, რა შემთხვევაშიც მოწმობის მფლობელს მოეთხოვება, შეიყვანოს საიდუმლო $PIN_{sig}$.

6.4. ღია გასაღებით დაშიფრული მნიშვნელობის გაშიფვრა დაშიფრული მნიშვნელობის და შესაბამისი დახურული გასაღების გამოყენებით, რა შემთხვევაშიც მოწმობის მფლობელს მოეთხოვება, შეიყვანოს საიდუმლო $PIN_{auth}$.

## 4.8 ზოგადი მოთხოვნები დოკუმენტის ბლანკის წარმოებისა და მიწოდების მიმართ

1. ბლანკების წარმოების დროს მომწოდებელი უნდა მოქმედებდეს ISO 14298:2013 ან ეკვივალენტური სტანდარტის მოთხოვნების შესაბამისად. ბლანკების დამამზადებელი საწარმო სერტიფიცირებული უნდა იყოს ISO 14298:2013 ან ეკვივალენტური სტანდარტის მოთხოვნების შესაბამისად და იძლეოდეს გარანტიას, რომ სერტიფიკატი ვალიდური იქნება კონტრაქტის მთელი მოქმედების ვადის განმავლობაში.

2. მომწოდებელმა უნდა უზრუნველყოს სრული ანგარიშგება და მიკვლევადობა დოკუმენტების ბლანკების წარმოების დროს გამოყენებულ დამცავ მასალებთან მიმართებით, მათ შორის, წარმოების პროცესში გაფუჭებულ დეფექტურ ბლანკებთან მიმართებითაც და ამ მიზნით იქონიოს შესაბამისი სააღრიცხვო სისტემა და განახორციელოს სრული ურთიერთშედარება წარმოების პროცესის თითოეულ ეტაპზე. ბლანკების წარმოების დროს გამოყენებული თითოეული დამცავი მასალისათვის უნდა დგებოდეს დეტალური აუდიტორული ანგარიში. აღნიშნული ანგარიშები რეგულარულად უნდა მოწმდებოდეს დამოუკიდებელი აუდიტორების მიერ, რომლებიც არ იქნებიან უშუალოდ ჩართული წარმოებისა და მარაგის აღრიცხვის პროცესში. აუცილებელია შეიქმნას და შენახული იქნას დოკუმენტები დამცავი მასალების ნაშთისა და დეფექტური ან

წარმოების პროცესში გაფუჭებული ბლანკების განადგურების შესახებ, რომელიც დადასტურებული იქნება ზედამხედველობაზე პასუხისმგებელი მაღალი რანგის თანამდებობის პირის მიერ.

3. სააგენტოს უფლებამოსილ წარმომადგენლებს უფლება აქვთ, შეამოწმონ მომწოდებლის წარმოების ცენტრის შესაბამისობა ტექნიკური დავალებით განსაზღვრულ მოთხოვნებთან და, შესაბამისი პროცედურების პრაქტიკაში დაცვის ხარისხი (მაგ., მასალების შენახვა, აღრიცხვა და გამოყენება). დაგეგმილი შემოწმების ჩატარების შესახებ სააგენტოს წარმომადგენელმა უნდა აცნობოს მომწოდებელს წარმოების ცენტრში სავარაუდო ვიზიტამდე 1 (ერთი) სამუშაო დღით ადრე მაინც. მომწოდებლის წარმომადგენელი ვალდებულია, შეადგინოს წერილობითი ანგარიში წარმოების ცენტრში ვიზიტის და ჩატარებული შემოწმებების შესახებ, რომელსაც ხელს მოაწერენ სააგენტოსა და მომწოდებლის წარმომადგენლები. თუ მომწოდებლის წარმომადგენელი უარს იტყვის ანგარიშის ხელმოწერაზე დასაბუთებელი მიზეზის გარეშე, ანგარიში ჩაითვლება ხელმოწერილად. ანგარიში წარმოადგენს შესაბამისი ვალდებულებების დარღვევის დროს (ასეთის დადგენის შემთხვევაში) პრეტენზიების წარდგენის საფუძველს.

4. ბლანკების წარმოებისას გამოყენებული მასალები აღებულ უნდა იქნეს კონკრეტული დაცული პროდუქტისათვის შექმნილი შეზღუდული ასორტიმენტიდან და შესყიდულ უნდა იქნეს მხოლოდ დამცავი მასალების სანდო და სერტიფიცირებული მომწოდებლებისგან. სატენდერო წინადადებაში პრეტენდენტმა უნდა ჩამოთვალოს ყველა მომწოდებელი, ვისგანაც იგი შეიძენს ბლანკების წარმოებისათვის საჭირო მასალებს ან/და კომპონენტებს. მომწოდებლების ცვლილება შესაძლებელია მხოლოდ სააგენტოსთან შეთანხმებით, რომელიც არ არის უფლებამოსილი, უსაფუძვლოდ უარჰყოს ასეთი ცვლილება.

5. მომწოდებელი ვალდებულებას იღებს, რომ წარმოების პროცესში, ხელშეკრულების მოქმედების მთელი ვადის განმავლობაში უზრუნველყოს ნედლეულის, შუალედური პროდუქტებისა და საბოლოო პროდუქტის ხარისხის სრული კონტროლი.

6. წარმოებული ან/და შესყიდული ბლანკის ხარისხის შემოწმება უნდა ეფუძნებოდეს მის სპეციფიკაციას, ბლანკის ნიმუშს და სააგენტოს მიერ დამტკიცებულ ბლანკების ხარისხიდან დასაშვები გადახრის კატალოგს. სატენდერო წინადადებაში მომწოდებელმა მოკლედ უნდა აღწეროს კომპანიის პრაქტიკა ხარისხიდან დასაშვები გადახრების კატალოგის შემუშავების კუთხით და მოიყვანოს ხარისხიდან დასაშვები და დაუშვებელი გადახრების მაგალითები. სააგენტო უფლებამოსილია, არ დაამტკიცოს ხარისხიდან გადახრა, რომელიც ეხება ბლანკის დეფექტს ფოტოსურათის ინტეგრირების არეში, მანქანაკითხვად ზონაში (თუ ეს შექმნის პრობლემებს დოკუმენტის ოპტიკური წაკითხვის დროს), ბიომეტრიული მონაცემების ველებში და ასევე, დამცავ ნიშნებს (თუ ეს წარმოშობს ეჭვს დოკუმენტის სიყალბესთან დაკავშირებით).

7. ბლანკები მიწოდებულ უნდა იქნეს სააგენტოს ოფისში მდებარე მისამართზე: საქართველო, თბილისი, აკაკი წერეთლის გამზირი, #67ა, Incoterms-ის DDP (მიწოდება განბაჟებით) პირობის შესაბამისად. პერსონალიზაციის ცენტრებისთვის განკუთვნილი აპარატურა სააგენტოს უნდა მიეწოდოს წინამდებარე სატენდერო დოკუმენტაციით განსაზღვრულ მისამართებზე თბილისში, ქუთაისსა და ბათუმში, DDP, Incoterm 2010-ის საფუძველზე (მიწოდება განბაჟებით).

8. მიწოდებული ბლანკები (ელექტრონული პასპორტი და პირადობის ელექტრონული მოწმობა) უნდა იყოს ქარხნულად დანომრილი ტექნიკური დავალების მოთხოვნების შესაბამისად. დანომვრის სქემა უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

8.1. ყველა დოკუმენტს უნდა ჰქონდეს უნიკალური ნომერი. დაუშვებელია ერთი და იმავე ნომრის მინიჭება სხვადასხვა ტიპის ორი დოკუმენტისათვის.
8.2. მნიშვნელობა უნდა იყოს ანბანურ-ციფრული. პირველი ორი სიმბოლო უნდა აღნიშნავდეს ბეჭდვის წლის ბოლო ორ ციფრს.
8.3. დოკუმენტის ნომერი არ უნდა შეიცავდეს სამი 6-იანის თანმიმდევრობას (ასე რომ, გამოტოვებულ უნდა იქნეს ყველა რიცხვი, რომელიც შეიცავს ნომერს „666“).

9. ბლანკები უნდა შეიფუთოს მომწოდებლის წარმოების ცენტრში ისე, რომ:
9.1. ადვილი შესამჩნევი იყოს პაკეტების უნებართვოდ გახსნის მცდელობა;
9.2. თითოეული პაკეტის წონა არ აღემატებოდეს 15 კგ-ს;
9.3. მხოლოდ სააგენტოს მხრიდან მოთხოვნის შემთხვევაში, გარე შეფუთვაზე დატანილ უნდა იქნეს პაკეტის შიგთავსის შესახებ ინფორმაცია.
9.4 ბლანკები იმგვარად უნდა იყოს მოთავსებული ხის ყუთებში, რომ გამოირიცხებოდეს ბლანკების დაზიანება მისი შენახვისა და ტრანსპორტირების დროს.

10. ტვირთს თან უნდა ახლდეს სააგენტოს მიერ განსაზღვრული მოთხოვნების შესაბამისი დოკუმენტები (ანგარიშფაქტურა შესაბამისი ინფორმაციით, ტვირთში არსებული ბლანკების ნუსხა, მათი ტიპი და დოკუმენტის ნომრები (ნომრების დიაპაზონი), ასევე ელექტრონული ფაილი ბლანკების ნომრების და შესაბამის ბლანკებში ჩაშენებული მიკროსქემების იდენტიფიკატორების მითითებით). ზემოხსენებული თანმხლები დოკუმენტები ელექტრონული ფორმით უნდა გაეგზავნოს სააგენტოს ტვირთის მიღების დაგეგმილ თარიღამდე, მინიმუმ, 3 (სამი) სამუშაო დღით ადრე. დოკუმენტების ფორმა განისაზღვრება კონტრაქტის გაფორმების შემდეგ.

11. ბლანკების ტრანსპორტირებისას დაცული უნდა იყოს ფასეული ტვირთის გადაზიდვისათვის დაწესებული მოთხოვნები, მათ შორის:
11.1. ტვირთს უნდა იცავდეს უსაფრთხოების პერსონალი;
11.2. გადამზიდ კომპანიას უნდა ჰქონდეს უნაკლო რეპუტაცია და გამოცდილება ფასეული ტვირთის გადაზიდვის სფეროში;

11.3. ტვირთის ზუსტი ადგილმდებარეობის განსაზღვრა (თრექინგი) და წვდომა მომწოდებლის და სააგენტოს მიერ ნებისმიერ დროს.

12. სააგენტოს მიერ დოკუმენტების მიღების შემდეგ ჩატარდება შემდეგი სახის შემოწმება:

12.1. შეფუთვის შემოწმება ტრანსპორტირების დროს უნებართვო გახსნაზე;

12.2. მიღებული ბლანკების ნომრების შემოწმება;

12.3. შეფუთვის დაზიანების ან/და რაიმე სხვა შეუსაბამობის გამოვლენისას დგება შესაბამისი აქტი და აღნიშნულის შესახებ დაუყოვნებლივ ეცნობება მომწოდებელს.

13. სააგენტოს მხრიდან მოთხოვნის შემთხვევაში, მომწოდებელი ვალდებულია დაუსაბუთებელი შეფერხების გარეშე მიაწოდოს სააგენტოს ბლანკების პერსონალიზაციისათვის საჭირო ყველანაირი ინფორმაცია (მათ შორის და არა მხოლოდ პერსონალიზაციის მანქანებთან კომუნიკაციის პროტოკოლის აღწერა, წარმოების პროცესისათვის ნებისმიერი სპეციფიკური მოთხოვნა და ნებისმიერი ინფორმაცია, რისი ცოდნაც სააგენტოს დასჭირდება პერსონალიზაციის პროცესის ასაწყობად და განსახორციელებლად).

14. თუ შესყიდვის ობიექტი (#1 ცხრილში განსაზღვრული ნებისმიერი დოკუმენტი) შეიცავს სააგენტოს პერსონალიზაციის დროს განსახორციელებელ რაიმე უსაფრთხოების ზომას (მაგ., გამჭვირვალე სტრუქტურის პერსონალიზება, მფლობელის პერსონალური მონაცემების რელიეფური ამოტვიფვრა და სხვ.), მომწოდებელმა ასევე უნდა განახორციელოს პერსონალიზაციის აღჭურვილობის კონფიგურირება, რათა უზრუნველყოს ასეთი უსაფრთხოების ზომის სათანადო გამოყენება და მიაწოდოს ნებისმიერი საჭირო ინფორმაცია სააგენტოს, რაც შეიძლება დასჭირდეს პერსონალიზაციის სისტემის კონფიგურირებისათვის.

15. მომწოდებელი ვალდებულია, უზრუნველყოს პირადობის ელექტრონული მოწმობისა და ელექტრონული პასპორტისათვის შეთავაზებული ელექტრონული კომპონენტების (ჩიპის, ოპერაციული სისტემისა და აპლიკაციების) უსაფრთხოების სერტიფიცირება წინამდებარე დოკუმენტით განსაზღვრული მოთხოვნების შესაბამისად და, საჭიროებისამებრ, ხელახალი სერტიფიცირება ხელშეკრულების მოქმედების მთელი ვადის განმავლობაში. თუ რომელიმე კომპონენტი დაკარგავს სერტიფიცირების სტატუსს, მომწოდებელი ვალდებულია, დაუსაბუთებელი შეფერხების გარეშე შეატყობინოს სააგენტოს აღნიშნულის შესახებ და მიიღიოს ყველა საჭირო ზომა სერტიფიცირებული კომპონენტების მიწოდების გასაახლებლად.

16. სააგენტოს მიერ ხარვეზიანი ბლანკების გამოვლენის შემთხვევაში/შემთხვევებზე რეაგირების მიზნით (ხარვეზები, რომლებიც გამოწვეულია მომწოდებლის მიზეზით), სულ მცირე, 6 (ექვსი) თვეში ერთხელ უნდა შედგეს აქტი, რომელსაც ხელს მოაწერენ სააგენტოს და მომწოდებლის უფლებამოსილი წარმომადგენლები.

17. ხარვეზიან ბლანკებს განკარგავს სააგენტო.

18. მომწოდებელს ხარვეზიანი ბლანკები არ უბრუნდება, გარდა იმ შემთხვევისა, როდესაც გამოსაძიებელია ხარვეზის მიზეზი. ხარვეზიანი ბლანკების დაბრუნება შესაძლებელია მხოლოდ სააგენტოს თანხმობით.

19. მომწოდებელმა სააგენტოს უნდა მიაწოდოს ხარვეზიანი ბლანკების რაოდენობის შესაბამისი ბლანკების დამატებითი რაოდენობა ბლანკების მომდევნო დაგეგმილ პარტიასთან ერთად ან აუნაზღაუროს ხარვეზიანი ბლანკების ღირებულება სააგენტოსთვის გაცემული მომდევნო ანგარიშფაქტურის ღირებულებიდან შესაბამისი თანხის დაქვითვის გზით.

20. პირადობის დამადასტურებელ დოკუმენტებზე (პასპორტები, პირადობის მოწმობები და სხვ.) არსებული ფაქტობრივი მოთხოვნიდან გამომდინარე, სააგენტოს უნდა შეეძლოს, ბლანკების მიწოდების დაგეგმილ ან მოთხოვნილ თარიღამდე, მინიმუმ, 6 (ექვსი) თვით ადრე შეიტანოს ცვლილებები მიწოდების გრაფიკში.

## 4.9 დოკუმენტების პერსონალიზაცია

### 4.9.1 ზოგადი პრინციპები

1. პერსონალიზაციის მართვის პროგრამული უზრუნველყოფას შეიმუშავებს სააგენტო. ერთი პერსონალიზაციის სისტემით განხორციელდება როგორც მოწმობების, ისე პასპორტების პერსონალიზაციის პროცესის მართვა. ყველა ადმინისტრაციული ფუნქცია (მარაგები, სამუშაო დავალება და სხვ.) საერთო იქნება ორივე დოკუმენტისათვის. სერვერები, ისევე როგორც უსაფრთხოების აპარატურული მოდულები (HSMs) კრიპტოგრაფიული ოპერაციებისათვის უზრუნველყოფილი იქნება სააგენტოს მიერ.
2. მიმწოდებელმა უნდა უზრუნველყოს აპარატურის მიწოდება (აპარატურის აღწერილობითი დოკუმენტაციისა და მისი კონფიგურირების სახელმძღვანელოების თანხლებით ინგლისურ ან ქართულ ენაზე), რომელიც საჭიროა:
   - 2.1. ელექტრონული პასპორტების პერსონალიზაციისათვის;
   - 2.2. პირადობის ელექტრონული მოწმობების პერსონალიზაციისათვის;
   - 2.3. პერსონალიზაციის მანქანების გაფართოებების შემუშავებისა და ტესტირებისათვის, რაც ითვალისწინებს, სულ მცირე შემდეგს:
     - 2.3.1. ჩიპის კოდირებას (კონტაქტური და უკონტაქტო);
     - 2.3.2. ლაზერული ამოტვიფვრის ემულირებას (მის ნაცვლად გამოსახულების ფაილების შექმნას);
   - 2.4. PIN/PUK კონვერტების საბეჭდი მანქანები (mail finisher) (იხ. თავი 4.9.7);
   - 2.5. კონვერტში ჩამდები მანქანები (იხ. თავი 4.9.8).

3. მომწოდებელი პასუხისმგებელია პერსონალიზაციის მანქანების შიდა პარამეტრებისა და პროგრამული უზრუნველყოფის სრულად კონფიგურირებაზე შესყიდვის ობიექტის (#1 ცხრილით განსაზღვრული დოკუმენტის ბლანკების) პერსონალიზაციის მხარდასაჭერად ისე, რომ პროცესი არ საჭიროებდეს ჩარევას სააგენტოს პერსონალის მხრიდან, ან საჭიროებდეს მინიმალური დოზით.
4. სააგენტო გეგმავს, განახორციელოს ხარისხის კონტროლი მანქანების შიგნით და გარეთ. მანქანის გარეთ ხარისხის კონტროლის განსახორციელებლად, მიწოდებულ უნდა იქნეს ხარისხის კონტროლის პროგრამული უზრუნველყოფის ბიბლიოთეკა.
5. მე-2 პუნქტის მოთხოვნების შესაბამისად მიწოდებული ყველა სახის აპარატურა უნდა იყოს მომწოდებლის საკუთრებაში და მფლობელობაში უნდა გადაეცეს სააგენტოს, ხოლო სააგენტოს უნდა დაევალოს, დაიცვას მომწოდებლის მიერ განსაზღვრული აპარატურის ექსპლუატაციის წესები. კონტრაქტის ამოწურვიდან არაუგვიანეს 6 (ექვსი) თვის შემდეგ, მომწოდებელი ვალდებულია, სააგენტოს მეთვალყურეობით უსაფრთხოდ წაშალოს პერსონალიზაციის მანქანებიდან ყველა მგრძნობიარე (სენსიტიური) ინფორმაცია და გაიტანოს აპარატურა სააგენტოს კუთვნილი შენობებიდან.
6. იმისათვის, რომ სააგენტოს მიეცეს პერსონალიზაციის სისტემის საკუთარი ძალებით განვითარების შესაძლებლობა, მომწოდებელი ვალდებულია, სააგენტოს პერსონალს ჩაუტაროს ტრენინგები. სააგენტოს მიერ არჩეულ, მაქსიმუმ, 50 (ორმოცდაათი) თანამშრომელს ჩაუტარდება, სულ მცირე, 40-საათიანი (ორმოცსაათიანი) ტრენინგები შემდეგ საკითხებზე (დეტალური დღის წესრიგი და მეცადინეობებზე განაწილება შეთანხმდება მომწოდებელსა და სააგენტოს შორის):
    6.1. მანქანების არქიტექტურა;
    6.2. მანქანების ყოველდღიური მოვლა და პრობლემების დიაგნოსტიკა;
    6.3. ახალი დოკუმენტის ტიპების დანერგვა, მათ შორის:
        6.3.1. ლაზერის სქემის გაუმჯობესება, ახალი სქემების განსაზღვრა;
        6.3.2. კონტაქტური და უკონტაქტო კოდირება;
        6.3.3. მანქანური მხედველობა;
        6.3.4. მანქანის შიგნით ხარისხის კონტროლი.
7. არაუგვიანეს ტრენინგების დასრულებისა, მომწოდებელი ვალდებულია, მიაწოდოს სააგენტოს ტრენინგის შესახებ ინგლისურ ან ქართულ ენაზე შედგენილი მასალა, სულ მცირე, ელექტრონული ფორმით.
8. მომწოდებელმა არ უნდა აუკრძალოს სააგენტოს წინამდებარე თავის თანახმად მიწოდებული აპარატურის სააგენტოს შეხედულებისამებრ, #1 ცხრილში განსაზღვრული დოკუმენტებისგან განსხვავებული დოკუმენტების პერსონალიზაციისათვის გამოყენება. იმის გათვალისწინებით, რომ დოკუმენტების ზომა და ფორმა შესაბამისი იქნება მანქანის სპეციფიკაციებთან, და მასალა, რომლებზეც განხორციელდება ლაზერული გრავირება, დააკმაყოფილებს შესაბამისი მანქანების მწარმოებლის რეკომენდაციებს. მომწოდებელმა არ უნდა მოითხოვოს დამატებითი ხარჯები და ღირებულება სააგენტოსაგან, გარდა პერსონალიზაციისას გამოყენებული მელნების ღირებულებისა (თუ გამოიყენება).

### 4.9.2 პერსონალიზაციის ცენტრები და მათი წარმადობა

1. პირველ ცხრილში განსაზღვრული ყველა ტიპის დოკუმენტის (ელექტრონული პირადობის მოწმობისა და ელექტრონული პასპორტის) პერსონალიზაცია განხორციელდება სამ სხვადასხვა ცენტრში:

1.1. თბილისის - სანაპიროს ქუჩა 2, თბილისი, საქართველო;

1.2. ქუთაისი - ირაკლი აბაშიძის ქუჩა 20, ქუთაისი, საქართველო;

1.3. ბათუმი - შერიფ ხიმშიაშვილის 7, ბათუმი საქართველო.

2. დანართებში მითითებულია პერსონალიზაციის ცენტრების გეგმები. მომწოდებელი ვალდებულია, პერსონალიზაციის აპარატურის მიწოდებისას გაითვალისწინოს პერსონალიზაციის ცენტრების სამუშაო ოთახების ფართობი და დაგეგმარება და აპარატურის მიწოდებამდე შეუთანხმოს მათი განლაგება სააგენტოს. სააგენტოს უფლება აქვს, უარი განაცხადოს შემოთავაზებულ განლაგებაზე, თუ იგი არ უზრუნველჰყოფს სააგენტოს პერსონალის ნორმალურ სამუშაო პირობებს.

3. პერსონალიზაციის აღჭურვილობა ადაპტირებული უნდა იყოს აღნიშნულ გარემო პირობებთან:

3.1. ელექტრობა - ცალფაზიანი 220 ვოლტი ან 3-ფაზიანი (380 ვოლტი, N, PE), 50 ჰერცი;

3.2. სხვა ტიპის დამატებითი საჭიროებების შემთხვევაში (როგორიცაა კომპრესირებული ჰაერი), მიწოდებულ უნდა იქნას ასეთი საჭიროების გენერირებისათვის საჭირო აღჭურვილობაც (მაგ. ჰაერის კომპრესორები) ყოველგვარი დამატებითი ხარჯისა და ღირებულების გარეშე.

4. თითოეულ ცენტრში არსებული მანქანები უნდა უზრუნველყოფდეს ქვემოთ მითითებულ მყისიერ საწარმოო სიმძლავრეს (სარეზერვო წარმადობის გამოყენების გარეშე), რომელიც გაიზომება ცალებით საათებში, იმის გათვალისწინებით, რომ პერსონალიზებულ დოკუმენტზე ძირითადი ფოტოს გარჩევადობა იქნება სულ მცირე 600 dpi ხოლო სხვა ოპტიკური მონაცემებისათვის - სულ მცირე 360 dpi:

| პერსონალიზაციის ცენტრი | მოწმობები | | პასპორტები | |
|---|---|---|---|---|
| | ნორმალური წარმოება (ერთი ცვლა, 7.5 სთ) | მაქსიმალური წარმოება (ორი ცვლა, 15 სთ) | ნორმალური წარმოება (ერთი ცვლა, 7.5 სთ) | მაქსიმალური წარმოება (ორი ცვლა, 15 სთ) |
| თბილისი | 180 ცალი საათში | 230 ცალი საათში | 160 ცალი საათში | 240 ცალი საათში |
| ქუთაისი | 65 ცალი საათში | 80 ცალი საათში | 55 ცალი საათში | 60 ცალი საათში |
| ბათუმი | 65 ცალი საათში | 70 ცალი საათში | 55 ცალი საათში | 60 ცალი საათში |

5. გადაუდებელ სიტუაციებში პერსონალიზაციის მანქანების სწრაფად შეცვლის მიზნით, მომწოდებელი ვალდებულია უზრუნველყოს, მინიმუმ 1 (ერთი) პასპორტის საბეჭდი მანქანისა და, მინიმუმ 1 (ერთი) პირადობის დამადასტურებელი მოწმობის საბეჭდი მანქანის (ან ერთი კომბინირებული საბეჭდი მანქანის) არსებობა თოთოეულ პერსონალიზაციის ცენტრში. დაკმაყოფილებულ უნდა იქნეს შემდეგი დამატებითი მოთხოვნები:

5.1. სარეზერვო მანქანების წარმადობა საკმარისი უნდა იყოს, რათა უზრუნველყოს შესაბამისი პერსონალიზაციის ცენტრის მუშაობა ნორმალური წარმოების შესაბამისი წარმადობით (პუნქტი 4) თუ მწყობრიდან გამოვა ერთი პერსონალიზაციის მანქანა;

5.2. მომწოდებელმა უნდა გაითვალისწინოს, რომ სააგენტო გამოიყენებს სარეზერვო მანქანებს ყოველდღიურ საქმიანობაში დაბალი დატვირთვით (მაგ., იმ დოკუმენტების დასაბეჭდად, რომლებიც იმავე დღეს უნდა გაიცეს), რათა უზრუნველყოფილ იქნეს მანქანის მუშა მდგომარეობა მუდმივად.

6. PIN/PUK კონვერტების საბეჭდი მანქანები (mail finisher), ისევე როგორც კონვერტში ჩამდები მანქანები, მიწოდებულ უნდა იქნეს ისე, რომ შეესაბამებოდეს პირადობის დამადასტურებელი მოწმობების პიკური წარმოების სიმძლავრეს (პუნქტი 4). სარეზერვო სიმძლავრის მიწოდება სავალდებულო არ არის.

### 4.9.3 მოთხოვნები პერსონალიზაციის აღჭურვილობის მიმართ

1. ლაზერული პერსონალიზაციის მანქანები უნდა უზრუნველყოფდნენ 700 dpi ან მეტ გარჩევადობას;

2. მოწმობის პერსონალიზაცია უნდა ხორციელდებოდეს 1 (ერთი) ციკლად (მათ შორის და არა მხოლოდ ლაზერული ამოტვიფვრა, მიკროსქემის კოდირება, ხარისხის კონტროლი), რაც გულისხმობს:

2.1. On board გასაღების გენერირებას;

2.2. სერტიფიკატების მომზადებას სააგენტოს მიერ ოპერირებულ PrimeKey EJBCA სისტემაში.

3. პასპორტის პერსონალიზაცია უნდა ხორციელდებოდეს 1 (ერთი) ციკლად (მათ შორის და არა მხოლოდ ლაზერული ამოტვიფვრა, მიკროსქემის კოდირება, ხარისხის კონტროლი).

4. ICAO-ს სტანდარტებთან სრული შესაბამისობის უზრუნველსაყოფად, ოპტიკური პერსონალიზაციის მოწყობილობა უნდა იძლეოდეს ინტეგრირებული კამერის სისტემის მხარდაჭერის საშუალებას მონაცემთა ველის დოკუმენტის კიდეებსა (მანქანაკითხვადი ზონის ხაზებისათვის) და გრაფიკულ ობიექტებთან პოზიციონირებისათვის.

5. პირადობის ელექტრონული მოწმობის პერსონალიზაციის მანქანაში ინტეგრირებული ე.წ. შემავალი თეფში (input tray) უნდა იტევდეს, მინიმუმ 200 (ორასი) მოწმობას.

6. პერსონალიზაციის აღჭურვილობა უნდა უზრუნველყოფდეს ინტეგრირებული სათვალთვალო სისტემის და გაფართოებადი ხარისხის კონტროლის პროგრამული უზრუნველყოფის მხარდაჭერას დოკუმენტზე ამოტვიფრული მონაცემების ნამდვილობის დასადგენად..

7. პერსონალიზაციის მანქანის შიდა პროგრამული უზრუნველყოფა მომწოდებლის მიერ უნდა გაიმართოს შემოთავაზებული შესყიდვის ობიექტის (#1 ცხრილით განსაზღვრული ბლანკების)

პერსონალიზაციისათვის. მას უნდა გააჩნდეს ქსელური ინტერფეისი, რომლითაც შემსყიდველის პროგრამულ უზრუნველყოფას ექნება შემდეგი შესაძლებლობა:

7.1 დოკუმენტ(ებ)ის ბლანკების პერსონალიზაციის მიზნით მანქანას გაუგზავნოს მოშორებული სისტემიდან ერთი ან რამდენიმე დავალება სტრუქტურირებულ ფორმატში (XML, JSON ან ASN.1). სააგენტოს უნდა მიეწოდოს #1 ცხრილით განსაზღვრული თითოეული ტიპის დოკუმენტის პერსონალიზაციისათვის საჭირო მონაცემების ნიმუში.

7.2 დოკუმენტის პერსონალიზაციის თითოეული ეტაპის დასრულების შემდეგ მოშორებულ სისტემაში მიიღოს დოკუმენტის სტატუსი, დოკუმენტზე დაბეჭდილ დოკუმენტის ნომერთან ერთად სტრუქტურირებულ ფორმატში. მიწოდებულ უნდა იქნეს მოშორებული სისტემის ნიმუში VmWare ვირტუალური სერვერის (appliance) ფორმით. ასევე მიწოდებულ უნდა იქნეს Java ან C# ენაზე დაწერილი შესაბამისი პროგრამული კოდი, რაც საშუალებას მისცემს შემსყიდველს, ხელახლა გამოიყენოს და შეცვალოს ის შეზღუდვის გარეშე.

8. დოკუმენტის პერსონალიზაციის შესაძლებლობები პერსონალიზაციის მანქანის შიგნით უნდა კონფიგურირდეს #1 ცხრილით განსაზღვრული თოთოეული ტიპის დოკუმენტისათვის, რაც მოიცავს შემდეგს:

8.1. ელექტრონული მატარებლის პერსონალიზაცია:

8.1.1. პერსონალიზაცია ელექტრონულ მატარებელთან APDU ბრძანებების გაცვლით, ასევე მონაცემთა გაცვლის მეშვეობით მოშორებულ სისტემასთან სტრუქტურირებულ ფორმატში (მაგ., JSON, XML ან ASN.1). სადემონსტრაციო მიზნებისთვის ნებადართულია თვითხელმოწერილი X.509 სტანდარტის სერტიფიკატების პირადობის ელექტრონულ მოწმობაზე გენერირებულ მომხმარებლის გასაღებებზე დისტანციური სისტემის მიერ გაცემა.

8.1.2. 8.1.1 პუნქტის საჭიროებების შესაბამისად, მიწოდებულ უნდა იქნეს დისტანციური სისტემის ნიმუში VmWare ვირტუალური აპლიკაციის ფორმით. ასევე მიწოდებულ უნდა იქნეს Java ან C# ენაზე დაწერილი შესაბამისი პროგრამული კოდი, რაც საშუალებას მისცემს შემსყიდველს ხელახლა გამოიყენოს და შეცვალოს ის შეზღუდვის გარეშე.

8.1.3. ჩაშენებულ ჩიპთან კომუნიკაციისათვის გამოყენებული უნდა იყოს უსაფრთხოების გასაღებების ნიმუშები, რომლებიც განსხვავდება შესყიდვის ობიექტისათვის (#1 ცხრილით განსაზღვრული დოკუმენტების, მათ შორის, დოკუმენტის ნიმუშებისთვის) გამოყენებული ნიმუშებისგან.

8.2. მანქანის შიგნით ხარისხის კონტროლის პროგრამულ უზრუნველყოფას უნდა შეეძლოს ბიოგრაფიული მონაცემების სიმბოლოებისა და მანქანაკითხვადი ზონის ოპტიკური ამოცნობა (ინგლისური და ქართული სიმბოლოების ჩათვლით) და უნდა კონფიგურირდეს ისე, რომ შეეძლოს #1 ცხრილში მითითებული დოკუმენტების პერსონალიზაციის პროცესში ლაზერით ამოტვიფრული მონაცემების შედარება დავალებაში მოცემულ მონაცემებთან. კონფიგურაცია გამოყოფილ უნდა იყოს ლაზერული ამოტვიფვრის შაბლონისგან, ისე რომ ლაზერულ შაბლონში ცვლილება მოითხოვდეს ცვლილებას ხარისხის კონტროლის კონფიგურაციაში.

9. მანქანა უნდა იყოს საკმარისად მოქნილი, რათა შემსყიდველმა, სურვილისამებრ, დაამატოს იმავე ფორმის სხვა დოკუმენტი (პასპორტის მანქანის შემთხვევაში - TD-3 ფორმატის, ხოლო პირადობის

მანქანის შემთხვევაში - TD-1 ფორმატის), რაც მოიცავს შავ-თეთრ ლაზერულ ამოტვიფვრას, ფერადი ფოტოს შექმნას #1 ცხრილში მითითებული დოკუმენტებისათვის შემოთავაზებული ტექნოლოგიით და ხარისხის კონტროლს. პირადობის მოწმობის მანქანის შემთხვევაში, უნდა შეიძლებოდეს როგორც კონტაქტური, ისე უკონტაქტო ინტერფეისის კოდირება შემდეგი დამატებითი მოთხოვნების გათვალისწინებით:

9.1. იმ შემთხვევაში, თუ მიკროსქემის კოდირებას ესაჭიროება მანქანისთვის გარკვეული დანამატის შემუშავება, ეს უნდა შეიძლებოდეს Java, C#, C, C++, Python ან JavaScript პროგრამირების ენაზე;

9.2. ლაზერული ამოტვიფვრა და ფოტოს შექმნა უნდა იყოს მარტივი და მოქნილი პროცესი, რომელიც შემსყიდველს ვიზუალური ელემენტების სასურველი განლაგების სქემის თავისუფლად არჩევის შესაძლებლობას მისცემს;

9.3. ხარისხის კონტროლი უნდა უზრუნველყოფდეს დამატებითი ფონტების დანერგვის შესაძლებლობას;

9.4. შესაძლებელი უნდა იყოს არჩევითობის პრინციპით ვიზუალური პერსონალიზაციის, ჩიპის კოდირების, ხარისხის კონტროლის და მათი ნებისმიერი კომბინაციის გამოყენება;

9.5. მანქანებთან ერთად მოწოდებულ უნდა იქნეს დოკუმენტაცია, რომელიც საშუალებას მისცემს შემსყიდველს, საკუთარი რესურსებით დანერგოს დამატებითი დოკუმენტის ტიპები.

### 4.9.4 მოთხოვნები ტექნიკური მხარდაჭერისა და მომსახურების მიმართ

1. პერსონალიზაციის პროცესში გამოვლენილი ხარვეზების მაქსიმალურად ოპერატიულად მოგვარებისთვის, მომწოდებელს უნდა ჰყავდეს ადგილობრივი (საქართველოში) მხარდაჭერის სერვისი, რომელსაც ექნება პირადობის დამადასტურებელი და სამგზავრო დოკუმენტების ტექნოლოგიური მხარდაჭერისა და ტექნიკური მომსახურების გამოცდილება. ტექნიკური მხარდაჭერა და შესაბამისი მომსახურება მომწოდებელმა უნდა უზრუნველყოს მანამ, სანამ სააგენტო არ დაბეჭდავს უკანასკნელ ბლანკს, მოწოდებულს მოცემული ტენდერის ფარგლებში დადებული კონტრაქტის მიხედვით.
2. მომწოდებელმა უნდა უზრუნველყოს ვებზე დაფუძნებული მხარდაჭერის პორტალის არსებობა, სადაც სააგენტო დაარეგისტრირებს ტექნიკური მხარდაჭერისა და მომსახურების მოთხოვნებს. სააგენტოს პერსონალის მიერ ინციდენტის რეგისტრაცია და კომენტირება უნდა დადასტურდეს მოთხოვნის დამრეგისტრირებელი პირისათვის ელფოსტაზე შეტყობინების გაგზავნის გზით, რომელშიც მითითებული იქნება ინციდენტის ტექსტი, რეგისტრაციის თარიღი და დრო. საჭიროებისამებრ, ამ პორტალის გამოყენებაში ჩართული უნდა იყოს სააგენტოს პარტნიორი ორგანიზაციები, სააგენტოს მოთხოვნის საფუძველზე.
3. კონტრაქტის მოქმედების ვადის განმავლობაში მომწოდებელი ვალდებულია, უფასოდ აღმოფხვრას პერსონალიზაციის პროცესში გამოვლენილი ნებისმიერი დადგენილი და დაფიქსირებული ხარვეზი (შეცდომა).

4. კონტრაქტის მოქმედების ვადის განმავლობაში მომწოდებელი ვალდებულია, უზრუნველყოს მიწოდებული კომპონენტების უფასო პროფილაქტიკური მომსახურება (მწარმოებლის განრიგის მიხედვით), უსაფრთხოების დროული განახლებების განხორციელება მიწოდებული ან შემუშავებული პროგრამული უზრუნველყოფისათვის და ასევე პროგრამული უზრუნველყოფის ოპერირება მხოლოდ იმ ოპერაციული სისტემის ვერსიებზე, რომლებიც მხარდაჭერილია ოპერაციული სისტემის დეველოპერის მიერ (რომლისთვისაც ხელმისაწვდომია უსაფრთხოების ,,პატჩები“).
5. საწყისი პრიორიტეტულობის დონე განისაზღვრება სააგენტოს მიერ შემდეგი მატრიცის მიხედვით:

| გავლენა | გადაუდებლობა | | | |
|---|---|---|---|---|
| | სასწრაფო | მაღალი | საშუალო | დაბალი |
| სააგენტოზე | 1-ლი დონე | 1-ლი დონე | მე-2 დონე | მე-3 დონე |
| დეპარტამენტზე | 1-ლი დონე | მე-2 დონე | მე-3 დონე | მე-3 დონე |
| ჯგუფზე | მე-2 დონე | მე-2 დონე | მე-3 დონე | მე-3 დონე |
| მომხმარებელზე | მე-3 დონე | მე-3 დონე | მე-4 დონე | მე-4 დონე |

6. თითოეული ინციდენტის პრიორიტეტულობა შეიძლება შეიცვალოს სააგენტოსა და მომწოდებელს შორის ორმხრივი შეთანხმების საფუძველზე ხელშეკრულების დადების შემდგომ. პრიორიტეტულობის დონის რიგითობის გაზრდის მოთხოვნის (გადაუდებლობის ან/და გავლენის შემცირების) შემთხვევაში მომწოდებელმა უნდა წარმოადგინოს სათანადო დასაბუთება.

7. რეაგირებისა და გადაჭრის დრო განისაზღვრება შემდეგნაირად (ინციდენტის გადაჭრის მაქსიმალური ვადის ათვლა დაიწყება ინციდენტის რეგისტრაციიდან):

| პრიორიტეტულობა | საპასუხო მოქმედების (რეაგირების) ვადა | ინციდენტის გადაჭრის მაქსიმალური ვადა | ტექნიკური მხარდაჭერის ხელმისაწვდომობა |
|---|---|---|---|
| 1-ლი დონე | 1 სთ. ან ნაკლები | არაუმეტეს 6 სთ-ისა | 9:00 – 18:00 თბილისის დროით |
| მე-2 დონე | 1 სთ. ან ნაკლები | არაუმეტეს 12 სთ-ისა | 9:00 – 18:00 თბილისის დროით |
| მე-3 დონე | 2 სთ. ან ნაკლები | არაუმეტეს 1 სამუშაო დღისა | 9:00 – 18:00 თბილისის დროით ორშაბათი - პარასკევი |

| | | | |
|---|---|---|---|
| მე-4 დონე | 4 სთ. ან ნაკლები | არაუმეტეს 3 სამუშაო დღისა | 9:00 – 18:00 თბილისის დროით ორშაბათი - პარასკევი |

8. თუ მომწოდებელს არ შეუძლია ინციდენტის გადაჭრა მე-7 პუნქტით განსაზღვრულ ინციდენტის გადაჭრის მაქსიმალურ ვადაში, მას უფლება აქვს მოითხოვოს ვადის გახანგრძლივება მოტივირებული დასაბუთებისა და ინციდენტის გადაჭრისათვის საჭირო დროის მითითების თანხლებით. განმარტება სააგენტოს უნდა წარედგინოს ხსენებული ვადის ამოწურვამდე, ხოლო სააგენტო, თავის მხრივ, ვალდებულია უპასუხოს მომწოდებელს დაუსაბუთებელი შეფერხების გარეშე. სააგენტოს მიერ ვადის გახანგრძლივების მოთხოვნის დადასტურების შემთხვევაში, ვადის გადაცილება არ ჩაითვლება დარღვევად და მომწოდებელს არ დაეკისრება ჯარიმები ვადის გადაცილებისათვის. ინციდენტის აღმოსაფხვრელად საჭირო მოქმედებები და ვადები განისაზღვრება ორმხრივი შეთახმების საფუძველზე.
9. პირველი და მე-2 დონის ინციდენტებისათვის სააგენტო უფლებამოსილი იქნება, მოითხოვოს მხარდაჭერის ხელმისაწვდომობის გახანგრძლივება დღეში 24 (ოცდაოთხი) საათამდე, 60 (სამოცი) დღის განმავლობაში 1 (ერთი) საკონტრაქტო წლის მანძილზე (წელი დაიწყება კონტრაქტის ხელმოწერის დღეს. არასრული წლის შემთხვევაში, დღეების რაოდენობა შემცირდება ხელმისაწვდომი დღეების პროპორციულად). სააგენტო უფლებამოსილი უნდა იყოს, მოითხოვოს მხარდაჭერის ხელმისაწვდომობის გახანგრძლივება პირველი დონის ინციდენტებისათვის ყოველგვარი წინასწარი შეთანხმების გარეშე. მომწოდებლის მიზეზით გამოწვეული ვადის გახანგრძლივება არ შეამცირებს 24-საათიანი მხარდაჭერისათვის განკუთვნილი დღეების რაოდენობას.
10. მე-7 პუნქტით განსაზღვრული ვადების დარღვევა გამოიწვევს ხელშეკრულებით განსაზღვრული ჯარიმების დაკისრებას.

### 4.9.5 გრაფიკული ელემენტების პერსონალიზაცია

#### 4.9.5.1 ძირითადი ფოტოსურათის პერსონალიზაცია ბარათისა და პასპორტისათვის

1. დოკუმენტის მფლობელის ძირითადი ფოტოსურათი უნდა იყოს ფერადი. საბაზო ზომა: სიმაღლე 40 (ორმოცი) მმ. და სიგანე 30 (ოცდაათი) მმ.; ზუსტი ზომა შეთანხმდება მომწოდებელსა და სააგენტოს შორის.
2. ფერადი ფოტოსურათი მიიღება პერსონალიზაციის დროს ლაზერული გრავირების ტექნოლოგიის მეშვეობით. დაუშვებელია ფოტოსურათის ჩაშენება პოლიკარბონატის კორპუსის (პირადობის ელექტრონული მოწმობის ან ელექტრონული პასპორტის მონაცემთა გვერდის) აწყობისას. უნდა დაკმაყოფილდეს შემდეგი დამატებითი მოთხოვნები:
   2.1. თუ ლაზერული გრავირებით მიიღება ფერადი ფოტო, აღარ უნდა მოხდეს ფოტოსურათის შემდგომი დამუშავება (მაგ. ლაზერის გარდა მელნის გამოყენება);

2.2. თუ ტექნოლოგია გულისხმობს შავ-თეთრი ფოტოს შექმნას ლაზერით, პოლიკარბონატის ზედაპირზე ჭავლური (inkjet) პრინტერით დატანილ უნდა იქნეს მელანი ისე, რომ მიღებულ იქნეს ფერადი ფოტო, არ გაფანტოს ყურადღება წარმოების დროს პოლიკარბონატის მასალაზე დატანილი დამცავი ნიშნებისგან და უზრუნველყოს ლაზერით ამოტვიფრული ფოტოსურათის ხილვადობა ინფრაწითელი ნათების ქვეშ. არ უნდა იქნეს გამოყენებული შავი მელანი და ყველა შავი ფერის ნაწილი უნდა იწარმოოს ლაზერის გამოყენებით.

2.3. ფოტოსურათის დაბეჭდვის შემდეგ აღარ უნდა მოხდეს დამცავი ფენის დატანა. 2.2. პუნქტის შესაბამისად ფოტოსურათის ბეჭდვის ტექნოლოგიის უსაფრთხოებისა და გამძლეობისათვის, ბეჭდვის პროცესი შეიძლება მოიცავდეს ჭავლური პრინტერის გამოყენებას პლიკარბონატის ზედაპირიდან ამოწეული პოზიტიური სტრუქტურების შესაქმნელად მხოლოდ შემდეგი მოთხოვნების დაკმაყოფილების შემთხვევაში:

2.3.1. ეს სტრუქტურები უნდა შეიცავდნენ ზედაპირულ რელიეფს;

2.3.2. პოლიკარბონატის ფენის ზემოთ ამოწეული ნაწილი უსაფრთხოდაა დაკავშირებული დოკუმენტის მფლობელის ფოტოსურათთან პირველი ან/და მე-2 დონის დამცავი ნიშნის/ნიშნების საშუალებით.

2.3.3. ლაზერით ამოტვიფრული ფოტოსურათი (იხ. პუნქტი 2.2) დაცული უნდა იყოს დიფრაქციული ოპტიკურად ცვლადი გამოსახულების გარდამქმნელით (Diffractive optically variable image device - DOVID), რომელიც ეფუძნება ნაწილობრივი მეტალიზაციის ტექნოლოგიას, უზრუნველყოფს გამჭვირვალობას მაღალი გარჩევადობით (შეიცავს 20 μm ან ნაკლები სისქის ხაზებს), შეიცავს პირველი, მე-2 და მე-3 დონის დამცავ ნიშნებს და განთავსებულია პირადობის ელექტრონული მოწმობისა და ელექტორნული პასპორტის მონაცემთა გვერდის იმ ფენაზე, რომელიც გამოიყენება ლაზერული ამოტვიფრისათვის.

2.4. მიუხედავად ფერადი ფოტოს ტექნოლოგიისა, ლაზერული ამოტვიფვრის შედეგად მიღებულ უნდა იქნეს წინამდებარე დოკუმენტით მოთხოვნილი გარჩევადობის მქონე (თავი 4.9.3. პუნქტი 1) სრული სახის ფოტოსურათი პოლიკაბონატში.

2.5. სააგენტოს უნდა მიეწოდოს ფოტოსურათის პერსონალიზაციის შემოთავაზებული ტექნოლოგისა და ასევე, დამატებითი უსაფრთხოებისა და გამძლეობის ზომების (მათ შორის ზომების, რომლებიც აკმაყოფილებენ 2.3. თავით განსაზღვრულ მოთხოვნებს, თუ გამოიყენება) დეტალური აღწერილობა, უსაფრთხოების კონცეფციის ჩათვლით, რომელიც უნდა მოიცავდეს რისკების ანალიზს პოტენციური საფრთხეებისა და სათანადო დამცავი მეთოდების მითითებით.

#### 4.9.5.2 პასპორტის სხვა ელემენტები

1. პასპორტის გრაფიკული პერსონალიზაცია უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

1.1. მოხდეს ტექსტური მონაცემებისა და MRZ (მანქანაკითხვადი ზონის) ჩვეულებრივი (შავ-თეთრი) ლაზერული გრავირება ;

1.2. მოხდეს გამჭვირვალე ან/და ნახევრად გამჭვირვალე სტრუქტურის ან/და ლინზისებრი ზონის (CLI, MLI ან მსგავსი ტექნოლოგია) ლაზერული გრავირება, ცვლადი მონაცემებით;

1.3. მიკროტექსტის გრავირება არ უნდა აღემატებოდეს 200 µm-ს მონაცემთა გვერდის ფონზე სრულყოფილად დაფიქსირებით;

1.4. დოკუმენტის წინა მხარეზე, სულ მცირე, ერთი გრაფიკული ელემენტის მოდიფიცირება უნდა მოხდეს რელიეფური ლაზერული გრავირების გზით;

1.5. ბარათზე წვდომის 6-ციფრიანი ნომერი (CAN) ლაზერულად უნდა ამოიტვიფროს მონაცემთა გვერდის წინა მხარეზე, ICAO-ს სტანდარტის შესაბამისად.

2. სტრუქტურას არ უნდა დაემატოს ზედა ფენა ან წებო, კერძოდ ზედა ფენა არ უნდა დაიტანებოდეს დოკუმენტის გრაფიკული პერსონალიზაციის შემდგომ.

#### 4.9.5.3 ბარათის სხვა ელემენტები

1. ბარათის გრაფიკული პერსონალიზაცია უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:
   1.1. მოხდეს ტექსტური მონაცემებისა და MRZ (მანქანაკითხვადი ზონის) ჩვეულებრივი (შავ-თეთრი) ლაზერული გრავირება ;
   1.2. მოხდეს გამჭვირვალე ან/და ნახევრად გამჭვირვალე სტრუქტურის ან/და ლინზისებრი ზონის (CLI, MLI ან მსგავსი ტექნოლოგია) ლაზერული გრავირება, ცვლადი მონაცემებით;
   1.3. მიკროტექსტის გრავირება არ უნდა აღემატებოდეს 200 µm-ს მონაცემთა გვერდის ფონზე სრულყოფილად დაფიქსირებით;
   1.4. დოკუმენტის წინა მხარეზე, სულ მცირე, ერთი გრაფიკული ელემენტის მოდიფიცირება უნდა მოხდეს რელიეფური ლაზერული გრავირების გზით;
   1.5. ბარათზე წვდომის 6-ციფრიანი ნომერი (CAN) ლაზერულად უნდა ამოიტვიფროს მოწმობის წინა მხარეზე, ICAO-ს სტანდარტის შესაბამისად.
2. სტრუქტურას არ უნდა დაემატოს ზედა ფენა ან წებო, კერძოდ ზედა ფენა არ უნდა დაიტანებოდეს დოკუმენტის გრაფიკული პერსონალიზაციის შემდგომ;

### 4.9.6 მანქანის გარეთ ხარისხის კონტროლი

1. მანქანის გარეთ ხარისხის კონტროლის გადაწყვეტილება მიწოდებულ უნდა იქნეს პროგრამული უზრუნველყოფის ბიბლიოთეკის სახით (საწყისი კოდის მოწოდება არაა სავალდებულო), რომლის ინტეგრირებაც შესაძლებელი იქნება სააგენტოს მიერ შემუშავებულ პერსონალიზაციის სისტემაში. მხარდაჭერილი უნდა იყოს Windows 7 ან უფრო ახალი ვერსია.

2. ხარისხის კონტროლის გადაწყვეტილება უნდა უზრუნველყოფდეს დოკუმენტის შემდეგი სკანერების მხარდაჭერას:

2.1. Regula;

2.2. Crossmatch.

3. ხარისხის კონტროლის ფუნქციაში შედის ქვემოთ ჩამოთვლილი ელექტრონული ჩიპების შიგთავსის შემოწმება:

3.1. DGs (EAC-ის შემდგომი DG3-ის ჩათვლით);

3.2. წვდომის კონტროლის მეთოდების მხარდაჭერა:

3.2.1. BAC;

3.2.2. Terminal Authentication;

3.2.3. PACE;

3.2.4. პასიური ავთენტიფიკაცია;

3..2.5. ჩიპის ავთენტიფიკაცია;

3.2.6. აქტიური ავთენტიფიკაცია.

4. გრაფიკული ელემენტების შემოწმება:

4.1. პერსონალური მონაცემები;

4.2. ხელმოწერა;

4.3. მანქანით წაკითხვადი ზონა;

4.4. ინფრაწითელი და ულტრაიისფერი სკანირება.

### 4.9.7 კონვერტის საბეჭდი მანქანები

1. სააგენტო მოითხოვს კონვერტის საბეჭდი მანქანების მიწოდებას PIN/PUK კონვერტების ლაზერული ბეჭდვის უზრუნველსაყოფად.
2. კონვერტის საბეჭდი მანქანა მიწოდებულ უნდა იქნას ქსელური ბეჭდვის შესაძლებლობის მქონე ზოგადი დანიშნულების მაღალი წარმადობის (შავ-თეთრ) ლაზერულ პრინტერთან მიერთებული ფორმით.
3. კონვერტის საბეჭდი მანქანა უნდა მუშაობდეს შემდეგი პრინციპების დაცვით:
   3.1. პრინტერს უნდა შეეძლოს მიღებული მონაცემების დაბეჭდვა A4 ზომის გვერდებზე (თერმული წებო დატანილი იქნება წინასწარ, თითოეულ გვერდზე).
   3.2. პრინტერი უსაფრთხოდ უნდა გადასცემდეს დაბეჭდილ ფურცელს დამლუქველს (sealer).
   3.3. დამლუქველმა მანქანამ 3-ად უნდა გაკეცოს და დალუქოს ფურცელი.

### 4.9.8 კონვერტში ჩამდები მანქანები

1. სააგენტოს ესაჭიროება კონვერტში ჩამდები მანქანები შემდეგი პროცესის ავტომატიზაციის მიზნით:
   1.1. PIN/PUK ჩანართის მოთავსება კონვერტში;
   1.2. A4 ფორმატის ფურცლების გაკეცვა და მოთავსება კონვერტში;
2. მხარდაჭერილი უნდა იყოს C6/5 (114 მმ x 29 მმ) ზომის კონვერტი.
3. მანქანებს უნდა შეეძლოთ კონვერტების დაწებება ან დაუწებებლად დატოვება მანქანის ოპერატორის მიერ არჩეული რეჟიმის შესაბამისად.

## 4.10 უსაფრთხოების გასაღებებისა და სხვა კონფიდენციალური მასალების მიწოდება

1. სააგენტომ და მომწოდებელმა უნდა გაცვალონ RSA-4096 ღია გასაღებები, რომლებიც თავსებადია GPG-სთან, შიგთავსის დაშიფვრის AES-256 გასაღებებით. სააგენტო საკუთარ გასაღებს მომწოდებელს გადასცემს კონტრაქტის გაფორმების შემდეგ. აუცილებელია, სულ მცირე, უსაფრთხოების გასაღების გაცვლის დაშიფვრა და ხელმოწერა ამ გასაღებების მეშვეობით. მომწოდებელს უფლება აქვს, ამ გასაღებით დაშიფროს ან/და მოაწეროს ხელი ნებისმიერ ინფორმაციას.
2. ელექტრონული მონაცემების დაშიფვრისა და ერთიანობის შემოწმებისათვის საჭირო გასაღებების მასალა სააგენტოს გადაეცემა დაშიფრული ფორმით ე.წ. „გასაღებების გაცვლის გასაღების“ მეშვეობით (KEK).
3. თუ სხვაგვარად არ შეთანხმდებიან სააგენტო და მომწოდებელი წერილობით, „გასაღებების გაცვლის გასაღების“ (KEK) გადაცემასთან დაკავშირებით იმოქმედებს შემდეგი მოთხოვნები:
   3.1. KEK უნდა იყოს 2TDEA, 3TDEA ან AES ტიპის;
   3.2. KEK უნდა დაიყოს 3 (სამი) ნაწილად, ისე რომ თითოეული ნაწილის სიგრძე იყოს საბოლოო გასაღების სიგრძის იდენტური და საბოლოო გასაღების დაანგარიშება შესაძლებელი იყოს მხოლოდ მაშინ, როცა ყველა ნაწილი იქნება ცნობილი;
   3.3. KEK-ის თითოეულ ნაწილს უნდა ჰქონდეს საკონტროლო მნიშვნელობა (KCV). ასევე, თავად KEK-ს უნდა ჰქონდეს ჯამური საკონტროლო მნიშვნელობა (KCV).
   3.4. გასაღების დაყოფის და KCV-ის გამოანგარიშების ალგორითმი უნდა შეირჩეს ისე, რომ სააგენტოს მიეცეს საშუალება, ჩატვირთოს ყველა გასაღები SafeNet ProtectServer External ტიპის აპარატურული უსაფრთხოების მოდულში (HSM), რომელსაც ის ამუშავებს, გამოიყენოს HSM-ის სტანდარტული შესაძლებლობები გასაღების ნაწილების შესაერთებლად და KCV-ის სისწორის გასაკონტროლებლად.
   3.5. ყველა გასაღების ყველა ნაწილი (მესამედი), რომლებიც ეკუთვნის KEK-ს, უნდა მიეწოდოს სააგენტოს მიერ დასახელებულ 3 (სამი) სხვადასხვა პირს. მიწოდება უნდა განხორციელდეს

მატერიალური ფორმით დალუქული კონვერტის მეშვეობით, რათა შესამჩნევი იყოს შესაძლო ხელყოფის მცდელობები. მიწოდება შეიძლება განხორციელდეს მომწოდებლის წარმომადგენლის მიერ პირადად, ან საფოსტო მომსახურებით.

3.6. KEK-ის ნაწილი არ უნდა გაეგზავნოს ადრესატს, სანამ წინა ნაწილის ადრესატი არ დაადასტურებს ნაწილის მიღებას.

4. ყველა სხვა გასაღები უნდა დაიშიფროს KEK-ის გამოყენებით, ხოლო შემდეგ - სააგენტოს GPG გასაღებით, რომლის გაცვლაც მოხდება პირველი პუნქტის შესაბამისად. დაშიფრული პაკეტი მიეწოდება სააგენტოს ელექტრონული ფოსტის საშუალებით. თითოეული გასაღები უნდა დაიშიფროს ისე, რომ სააგენტოს მიეცეს საშუალება, ჩატვირთოს ეს გასაღებები SafeNet ProtectServer External ტიპის აპარატურული უსაფრთხოების მოდულში (HSM) და იქვე, KEK-ის HSM-ის გარეთ გამოტანის გარეშე, გაშალოს (unwrap) ისინი.