Nummer-number	Vraag-Question:	Hoofdstuk- Chapter / paragraaf-Paragraph / bijlage-Annex	Antwoord-Answer:
1	De RFI beslaat 3 gebieden; 1. Aanleveren van een database tbv handmatige controle 2. Aanleveren van een database tbv machinale controle dmv bv een paspoort reader 3. Aanleveren van een invoermodule tbv de handmatige en machinale controle. Onze vraag: Heeft DMO het voornemen om tzt de 3 onderdelen van Basisvoorziening Echtheidskenmerken in 3 aparte percelen te zullen aanbesteden?		No. The preference of DMO lies in one supplier delivering all three parts of the system.
2	The RFI distinguishes between a Manual check (MC) and an Automated check (AC). In the context of the AC, reference is made to the chip in eMRTDs and verification of the electronic security features. Does the Ministry intend to design separate processes for automated checking of chip enabled eMRTDs compared to non-chip travel documents? I.e. is it acceptable to be “extra strict” on the physical security features of non-chip-enabled documents, and go for a higher performance for chip-enabled documents?		No, DMO does not intent to design separate processes for chip enabled and non-chip enabled documents because it is of the opinion that the checking of physical security features on chip-enabled documents is just as important as the checking of security features on non-chip enabled passports.
3	What system requirements (e.g. operating systems, redundancy, databases etc.) for both client application and servers do you have?	General System Requirements: Software	The target environment consists of Microsoft Windows based fileservers and Microsoft application servers. Redundancy will be provided by mirroring the operating environment.
4	What minimum hardware requirements must be supported by both client application software and server software?	General System Requirements: Hardware	DMO finds that this question is not yet relevant in this phase.
5	What kind and level of connectivity can be expected for each different scenario: MC, AC, and mobile inspection?	General Connectivity	For each scenario a service oriented approach is desired.
6	The RFI has not made any specific statements about requirements for software distribution and template database distribution. Could you describe your requirements for software distribution and software updates?	General Software / Database distribution	Software distribution (for example specific client software) and software updates will be deployed through standard Microsoft deployment.
7	It is not described what the overall expected system architecture is supposed to look like (e.g. Client application or Client/Server application scenario). Could you please provide such an overview and short description?	General Overall System Architecture	The overall expected system architecture is a Service Oriented Arhitecture with SOAP/XML messaging.

8	Grey box, first paragraph: “The BSSF has to be an integral information service that supports both the manual and automated checks of security features, and it serves to replace the current separate and limited applications.” What are the "current separate and limited applications"? Could you please list them and briefly explain their purpose and functionality?	Page 5 1.1	The current separate and limited applications serve only specific systems. An integral information service services all applications and has a central database.
9	Grey box, first paragraph: “The BSSF has to be readily available on a standard Ministry of Defence work station (both stationary and mobile).” Could you please specify a "standard Ministry of Defence work station (both stationary and mobile)" with regards to hardware and software?	Page 5 1.1	The applications must serve some platforms like a standard Intel based work station but also as a scalable application on Smartphone.
10	Section 3.1.1. states "On November 24 in 2015 all passports in circulation must include a MRZ. Section 4.1 states "It should be possible to find a fuzzy match using the reference data, especially when MRZ data is not available". Is our assumption correct that MRZ data will not (passport for all models) be available at the launch of the new BVE?	3.1.1	Yes, there is the possibility that there still will be passports in circulation without a MRZ at the launch of the new BSSF. Even if the launch is after 24 November 2015, this possibilty still exists because it is known that not all countries will be able to confirm to this ICAO-deadline.
11	Kan de inschrijver gebruik maken van bestaande gegevensverzamelingen van Defensie voor het vullen van de BVE?	3.1.2	No, because at the moment the Ministry of Defence does not have these types of data collections.
12	Is er een huidige database voor echtheidskenmerken voor handmatige controle en moet deze gemigreerd worden?	3.2.1	At the moment there is no intention of using a current database as a base for the new security features database.
13	Is er een huidige database voor echtheidskenmerken voor machinale controle en moet deze gemigreerd worden?	3.2.2	No, at the moment the Ministry of Defence does not have such a database.
14	controle echtheidskenmerken voor eerste, tweede en derde lijn. Bedoelt u dat er verschil is in de zichtbaarheid voor personen van de echtheidskenmerken?	H 4 - 4.1 /1.0 pag. 10	This is correct. In a Manual Check situation the amount of available reference images is based on the work environment (first, second, third line) and/or authorization (for example dependent on level of training or department).
15	Is het de bedoeling dat het aan en uitzetten van eerste, tweede en derdelijns echtheidskenmerken ook een rol spelen in het MC proces?	H 4 - 4.1 /1.0 pag. 10	No, there is no distinction in the automated checking of security features in first, second or third line control situations. However, there can be a distinction in the amount of feedback given to the user, depending on the work environment (for example not to overload the first line user with data).

16	U vraagt: "Welke van de genummerde functionaliteiten kunt u realiseren met uw product en op welke wijze?". In het voorbeeld plaatje staat ook 5.2, waar staat deze benoemd?	4.1.a	5.2 (Security Features Database) is part of the Content Module (CM) and is described in 4.4.
17	Is integration into MOD IT infrastructure (e.g. Active Directory) required in order to implement the authorization?	Page 10 4.1 1.0 Authorization Levels	Yes.
18	Bestaat er de wens/verwachting dat de eenvoudige handheld dmv ingebouwde IR en UV optiek de echtheidskenmerken van het document kan controleren? Indien dit het geval is; welke merk en type handheld zal u hierbij gaan gebruiken?	Pagina 11, bij punt 4.0	Checking of security features will follow the capabilities of the device. If IR or UV is not available on the device then it wil use the other (visual) capabilities. Which handheld device will be used is not known yet, acquisition of a new handheld is not within scope of this project. Existing equipment will be used.
19	What is your definition of the term “VIS response”? ICAO only defines what positions to check under IR and UV illumination to check for document paper.	Page 11 4.1 2.0 VIS response	The definition of VIS response here is an image in white (Visual) light (365-800 nm).
20	“…Tolerance in position blocks security features (text) block identification -…” Please elaborate on what kind of feature check you are expecting here.	Page 11 4.1 2.0.4	Even though security features and text blocks in documents have certain positions on the document, experience learns that these positions show some variation. This is especially true for personalization text blocks (for example name, place of birth, document number, etc.). A certain tolerance in identifying the position of these (text)blocks is therefore needed for them to be recognized as such.
21	Is the intention of this provision to be able to manually (i.e. by the operator) trigger a fuzzy search or do you expect such a search to automatically take place whenMRZ reading fails? What are the search criteria you expect to be supported?	Page 11 4.1 3.1 Fuzzy Search	A 100% selection on documenttypes based on MRZ readings is not guaranteed, hence a more advanced selection mechanism will be needed. We´d like to hear the suppliers suggestion for which fuzzy logic to use.
22	Please explain what exactly is meant by “using text blocks” here. Is there a difference in the AC functionality / behaviour in case it is used in the manned border control or if it is used in the SSPC?	Page 11 4.1 3.2 “For this application, the AC does not use text blocks	For the explanation of 'using text blocks', see the answer to question 20. Yes, there is a difference in behaviour. The central core of the security checking engine will interact with the userinterface returning validation of all the security attributes while the SSPC gets only a general "yes" or "No" from the security check engine.

23	Do you expect to include IR and UV checks in this scenario? If so, is it acceptable to use peripheral equipment, like e.g. UV lights?	Page 11 4.1 4.0 Mobile Checking	As explained in the answer to question 18, IR and UV checks in mobile applications are certainly a wish and preferably build in the hardware. Using peripheral equipment for Automated Check in this scenario is probably to complicated, but they could be used to assist the Manual Check of the document.
24	Is the tool meant to be used by MOD personnel or will MOD personnel provide new documents to the supplier to be added to the template database? Which reference database is currently being used and is it necessary to transfer data from this database to the new reference database?	Page 11 4.1 5.0 Content Module	The idea is indeed for the tool to be used by MOD personnel, which has a great deal of expertise on travel and identity documents and their security features. There is currently no standard reference database used for manual checks.
25	"De BVE HC bevat in ieder geval opnames met wit (VIS), ultraviolet op 365, 313 en 254 nm (UV) en infrarood licht (800 - >1000 nm)" Bestaat er de wens om de opnames van de echtheidkenmerken in de genoemde golflengtes eveneens uit te kunnen controleren met een Passport Reader (machinale controle)? UVB (315 - 280 nm) is nl in biologische zin over het algemeen de meest destructieve vorm van UV-straling omdat de energie hoog genoeg is om biologische weefsels rechtstreeks te beschadigen. Wij adviseren derhalve bij de machinale controle slechts gebruik te maken van UVA golflengte 365nm	Pagina 13, paragraaf 4.2	We agree. Due to health and safety issues, in Automated Checks (AC) UV-security features with a wavelength shorter than 365nm will not be checked.
26	First paragraph: “The BSSF MC is the part for support of manual security features checks and consists of a reference database.” Which reference database is currently being used and is it necessary to transfer data from this database to the new reference database?	Page 13 4.2	There is currently no standard reference database used for Manual Checks. The important thing is that through the BSSF a reference database will be readily available for use.
27	Each reader has different reading capabilities. The BSSF AC tests the security features within the possibility of the used reader or device. This means that the application has to be able to handle with the usual readers in the market and other devices. What is the expected behaviour of the checking system in case the device doesn’t support the checking of certain security features (e.g. the device doesn’t support the capturing of UV light images)?	Page 14 4.3	Depending on the hardware, the checking system will have to know which security features it is not able to check. The output of the check is based on the security features that the system is able to do. Besides, users should be well informed of what kind of checks the system they use is able to do, and what checks the system is not able to do.

28	Is this the expected behaviour for ICAO standardized documents only (more specifically the MRZ data page) or do you expect this behaviour also for non-MRZ documents (e.g. the front side of an ID card)?	Page 14 4.3 2. Standard Security Checks	With your question we assume you mean the behaviour of doing a minimum basic check according to ICAO-standards if the presented document is not yet entered in the database and is a non-MRZ document. However, we do not see an ID card as a non-MRZ document if the MRZ is printed on the back side. In this situation the back side could be scanned to do some basic checks, even if it is not entered in the database yet. For non-MRZ passports that are not entered in the database yet this is also true, but there will be less basic features to check. Besides, the chance of this happening will be small as worldwide all new passports have an MRZ.
29	U vraagt: "Welke mogelijkheden voor het lezen van elektronische echtheidskenmerken biedt uw oplossing en zijn deze naar behoefte te activeren?" Naar onze mening wordt er binnen de EKD oplossing helemaal niet gelezen. Lezen gebeurt ergens anders, bijvoorbeeld aan de grens, vanuit dat lezen zouden er electronische controles kunnen worden uitgevoerd door gebruik te maken van een inspectiesysteem. Bedoelt u om in de database vast te leggen welke vorm van electronische controle bij een document mogelijk is als echtheidskenmerk, of ziet u een document authenticatie rol van het EKD systeem? Kunt u dit verduidelijken?	4.3.d	There are two aspects on the BSSF eg. managing security features in the BSSF database and checking travel and identity documents against the content of the BSSF data. Both functionalities are part of the system.
30	Chapter 4.3 describes two functionalities: recognizing security features in the document (4.3c) and comparing security features (4.3g). On both features it states the same question. Is it correct that the demand on both functionality is the same? If not, what is the correct question per requested functionality?	4.3c, 4.3g	No, the functionality on both functionalities is not the same. 4.3c is about *recognizing* security features in order to find the right reference of the security features in the database. 4.3g is about the next step in checking the authenticity of these security features by comparing them to the reference found in the database. For further explanation and a change of 4.3g, see the answer to question 31.

31	Can you please explain your understanding of “checking”, “comparing” and “recognizing” security features?	Page 15 4.3 6. and 7., Questions 4.3f and 4.3g	Recognizing' a security feature means that the system is able to identify security features in order to be able to find the right reference of this security feature in the database (see answer to question 30). Based on this question and question 30, 4.3.6 and 4.3.7 will me merged into one paragraph (4.3.6) with one question (4.3.f): *4.3.6: Checking security features* *Functionalities for checking the authenticiry of security features by comparing the recognized security features with its corresponding reference images. For this part setting (dynamic) threshold levels and comparison algorithms are crucial.* *Question 4.3f Which methods and algorithms can you offer for checking the authenticity of different kinds of security features?*
32	Section 4.6.3. describes the minimal principles regarding the hardware. Is it expected that the BVE-solution should work on the current hardware(infrastructure) at the KMAR / MOD? Or will KMAR / MOD provide hardware, required to operate the BVE solution, as per specification of the supplier?	4.6.3	The answer to this question depends on the solution that is chosen, but using the current hardware is preferred.
33	On one hand, the “mobile” solution seems to imply a mobile capture device, but on the other hand it implies to be a scanner, tethered to some mobile device. Could KMar please elaborate on this?	4.6.3	The mobile solution is *not* intended to be a scanner tethered to some mobile device. In 4.6.3 it is indicated that VIS is the minimum requirement regarding the optical part for smart phones (an example of a mobile solution). The additional UV and IR lights are a minimum requirement for document readers.
34	The system should be able to support the current and valid hardware standards available in the market. Are there specific devices you are currently using or expect to be supported?	Page 18 4.6.3	No.

35	In het RFI wordt fuzzy matching verschillende malen genoemd.Wat voor soort data wordt er gebruikt in deze fuzzy matching? Namen, datums, document nummers? Biometrie en/of foto's? Of iets anders?	4.6.4	(see also remarks on question 21) A 100% selection on document types based on MRZ readings is not guaranteed, hence a more advanced selection mechanism will be needed. There is no prescription on which logic to use. We´d like to hear the suppliers suggestion for which fuzzy logic to use.
36	Waar dient gegevensset 2 voor, handmatige of machinale controle?	4.6.4	Data collection 2 serves the Manual Check, data collection 3 serves the Automated Check. All three data collections will form one database.
37	Text recognition software like OCR, which also recognizes date formats. Including possibilities to recognize Chines, Cyrillic, Greek or Thai characters and translate them into Latin script. Please further explain the expected behaviour. What Chinese character system do you expect to be supported?	Page 18 4.6.4	The system is expected to recognize and translate as much character systems that are used in official travel and identity documents as possible.
38	Please explain the figure in more detail. In certain parts of the document, the term “BVE” is used (e.g. pages 4, 10 and 19). Is this a currently existing system or is it the same as BSSF? What is the role of BVKMar in the architecture?	Page 19 4.6.5 Figure	BSSF is the English translation of its Dutch equivalent, the BVE. The overview BVKMar shows the future integration of components in a corporate KMar system.
39	Is data encryption required for all data captured/read from the document? Shall data transmission be done by secure messaging methods (e.g. SSL)? What security infrastructure is already provided by the MOD to secure the backend data?	Page 20 4.7 Data privacy	Information about security measures at the Ministry of Defence is confidential. Please elaborate on the security features of your product.
40	Chapter 4.9 DMO asks for an estimate of the costs (one-time and annual) for the realization and maintenance of the BVE. Can you please provide additional information about the range of the system in terms of number of users, number of user locations, number of (different) devices, number of templates of documents and number of models of passports (DMO mentioned in paragraph 3.1.1. a number of 5000)?	4.9.	At this stage DMO does not find the possible number of users, locations, and devices relevant.Thousands of documents will be checked every day. A number of 5.000 documents is indeed a first rough estimation of the number of models of passport models.
41	Hoeveel gebruikers verwacht Defensie met deze toepassing?	4.6.9a	See the answer to question 40.
42	Onder welke besturingssystemen dient de beoogde software te werken?		Intel based systems, Windows Operating system and Microsoft Application servers.