

WIPO



WIPO/DAS/PD/WG/2/2

ORIGINAL: English

DATE: June 29, 2007

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

E

WORKING GROUP ON THE DIGITAL ACCESS SERVICE FOR PRIORITY DOCUMENTS

**Second Session
Geneva, July 16 to 19, 2007**

SYSTEM ARCHITECTURE

Document prepared by the Secretariat

SUMMARY

1. A recommended system architecture is proposed with a view to ensuring that a suitable service can be delivered for applicants and Offices. The system would involve providing applicants with an access control code, allowing them to manage a list of Offices permitted to access a priority document before it has been made open to public inspection by the Office holding the document. A number of variations are possible in the means by which applicants are informed of the access control code: three entry routes are envisaged, permitting the system to work for Offices of first filing operating under different legal systems.

BACKGROUND

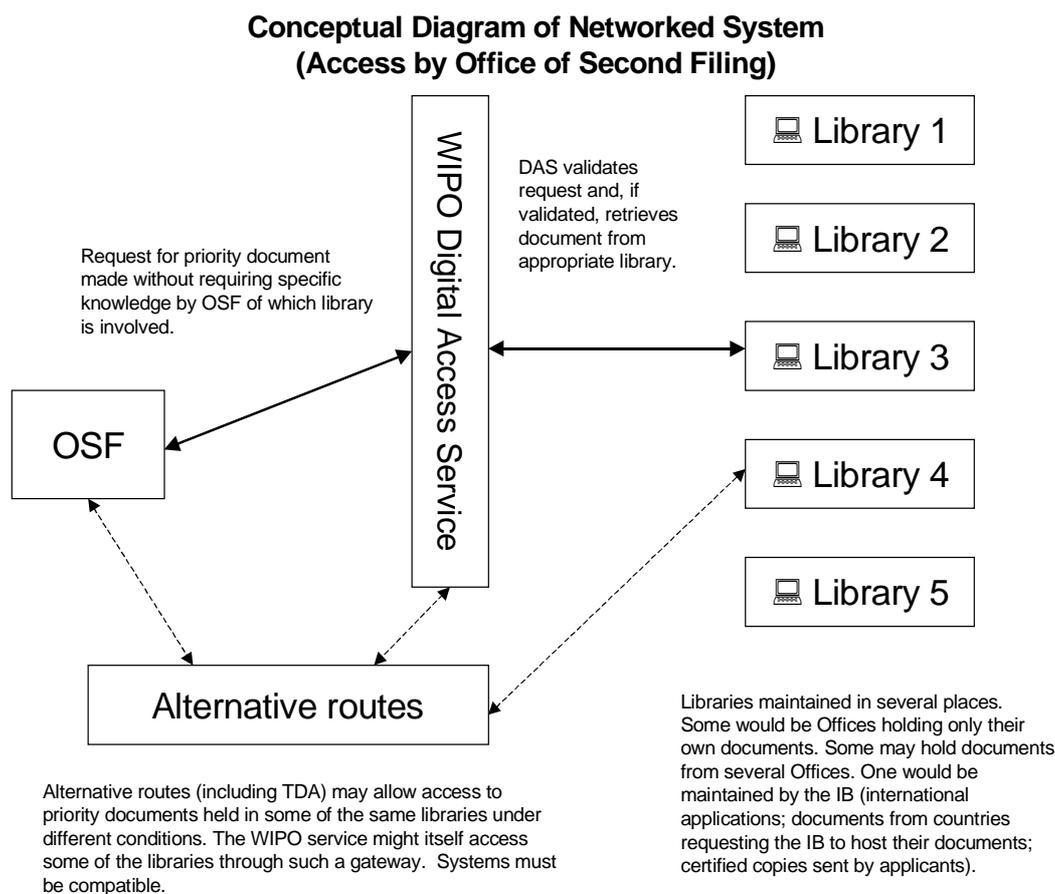
2. At its first session held in February 2007, the Working Group considered the system architecture of the proposed digital access service for priority documents. The report of the discussion at the session (see document WIPO/DAS/PD/WG/1/6¹, paragraphs 14 to 32) is reproduced for convenient reference in the Annex.

3. The first session of the Working Group made considerable progress in determining a network model for the digital access service (DAS). Central to this model was the

¹ Working documents and the electronic forum established to facilitate the work of the Working Group are accessible on WIPO's website via www.wipo.int/pdocaccess.

identification (amongst a number of agreed principles² for the network model) of a number of combinations of packaging channels and document formats that the system should handle (see paragraph 3 of the report in document WIPO/DAS/PD/WG/1/6, reproduced in the Annex to this document). Those combinations were seen as a means of enabling the International Bureau to make available priority documents securely accessible to Offices of second filing (OSFs) via PatentScope using a network of digital libraries, including WIPO's own digital library and the Trilateral Document Access (TDA) system as well as allowing for paper-based data flows. The network model is summarized in Figure 1, below, taken from the draft agreed principles set out in Annex II of document WIPO/DAS/PD/WG/2/3.

Figure 1



4. Following the first session of the Working Group, comments have been made by a number of delegations in informal discussions with the Secretariat. These were addressed particularly to possible ways of controlling access to priority documents that are not publicly available (see agreed principle no. 5 and paragraph 32 from the report of the first session, reproduced in the Annex). Following those discussions, the Secretariat now proposes a revised system of access control, which is illustrated in Figure 2, below. In cases where the system is able to determine that a priority document has been published (normally by the Office of first filing (OFF), but potentially by another Office or after confirmation by the applicant that the document should be publicly available), the access control mechanism

²

A slightly modified text of the agreed principles is proposed for approval by the Working Group as set out in Annex II of document WIPO/DAS/PD/WG/2/3.

would no longer be needed and it is envisaged that any Office would be able to access a document at that stage without the need for any authorization by the applicant.

KEY REQUIREMENTS OF AN ACCESS CONTROL SYSTEM

5. The revised system for access control will use an access control code and list of authorized Offices to drive the security and confidentiality requirements of the system. An access control code would be attributed to each priority document, and then used by the applicant to manage a list of Offices permitted to access the priority document securely within DAS. A number of key elements of the revised system for access control are required and envisaged:

- (a) the network model in Figure 1 should be supported;
- (b) it would permit certified copies of priority documents to be provided to DAS by the OFF, directly by applicants or by other Offices participating in DAS;
- (c) it must allow applicants to modify the access control code and the access control list using DAS at any time;
- (d) it must provide a means for applicants to authorize the disclosure of sufficient information to DAS (as would be needed in the case of certain Offices such as the United States Patent and Trade Mark Office);
- (e) it must provide to the OSF information on the dates that a priority document became available to DAS, and when the applicant authorized access to that OSF.

PROPOSED SYSTEM: MANAGED ACCESS LIST

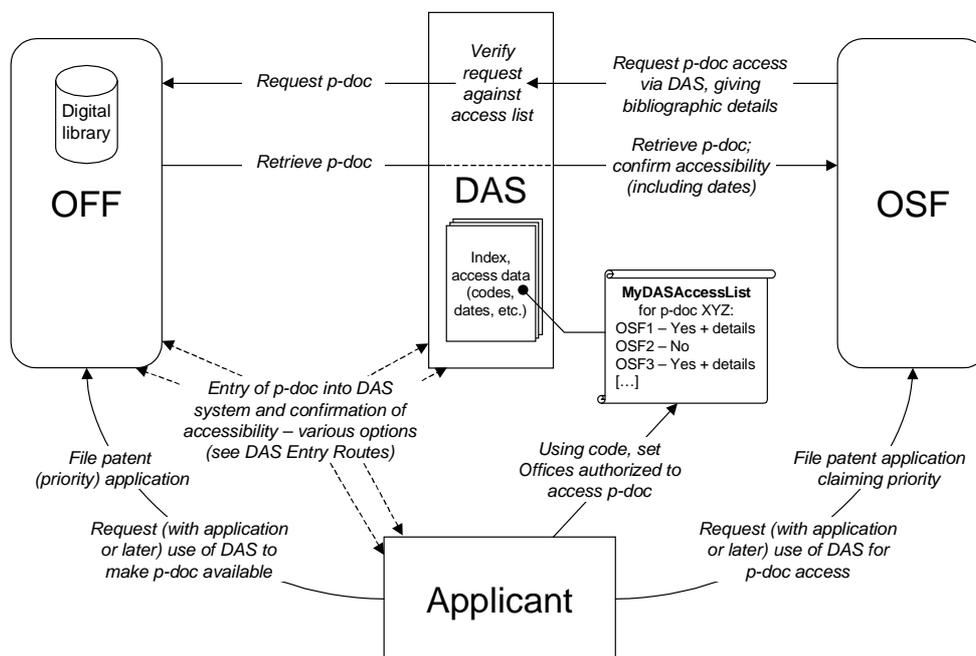
6. A preferred method is set out below, illustrated in Figure 2, for implementing such a system. The system is set out in terms of actions before an OFF, but in fact it would work in the same way where the relevant digital library is maintained by any Office which holds a certified copy of the priority document (for example, as an OSF), supplied by an agent or applicant for which the Office has a name and address and is therefore able to send the access control code to a person who is known to have the right to make use of the document.

7. It is proposed to take a “managed access list” approach to document access control. In this system, on requesting that an application that may later form the basis for a priority claim be made available through DAS, the applicant is allotted an access control code specific to the application. The system would support several different routes for entry of priority documents into the DAS system, allowing for different legal constraints and user requirements, as detailed below in paragraphs 13 and 14 and Figures 3 to 5.

8. Using the application number and the allotted code, the applicant can control which OSFs are permitted access to the application as a priority document by means of adjusting the settings in an access control list held in DAS by the International Bureau. This would normally be done directly by the applicant using a web interface, but for applicants with no Internet access, the International Bureau would set the details on request by post including the required information.

Figure 2

**DAS Access Control:
Applicant manages access lists**



9. When the later application claiming priority is made, the applicant would only need to state to a participating OSF that the priority document should be retrieved from DAS. The OSF would not require any information beyond the standard bibliographic details currently provided when making a priority claim in order to access the priority document, provided that access by that OSF had been authorized on the access control list within DAS for that priority document.

10. It should be noted that the step of authorizing access will be an essential one. Unless the applicant has set the authorization or the system recognizes that the document has already been published, the OSF will not be able to access the priority document through the system and rights might potentially be lost.

11. Possible future developments might include an “account” system, where an applicant who files many applications will be able to set a “default” access list, but this would not be part of the system to begin with in order to minimize costs and the time needed to deploy a basic working system.

Pros and cons of alternative access control systems

12. In reaching the above proposal for an access control system, a number of alternatives were considered. The main pros and cons of the proposed system and the other possibilities which were considered are outlined in the following table.

<i>System</i>	<i>Pros</i>	<i>Cons</i>
<p><u>“Security by obscurity”</u></p> <p>(no authorization required, beyond a participating Office having the relevant bibliographic details of an application which has been included in the system)</p>	<p>Very simple.</p>	<p>Insecure, both through hacking by guesswork and because some Offices publish bibliographic details of unpublished applications (including applications from other Offices from which priority has been claimed).</p> <p>Some applicants would be concerned and not use the system.</p> <p>Some Offices would not be prepared to participate because of risk of their improperly disclosing confidential material.</p>
<p><u>Access code for OSF use</u></p> <p>(issued by OFF or IB, to be given to any OSF to authorize access)</p>	<p>Good security in combination with obscurity and appropriate defenses against “brute force” attacks.</p> <p>Very easy to deal with assignments or different rights-holders for different States (code can simply be shared with other authorized applicants for different States).</p>	<p>Risk of incorrect transcription at several stages (applicant to assignee, applicant to OSF, OSF to DAS).</p> <p>Replacement of lost code might affect access to documents by OSFs already informed of the original code.</p> <p>Does not easily allow for development of system to permit uploading of priority documents.</p>
<p><u>Applicant-defined access code for OSF use</u></p> <p>(similar to above, but provided by applicant)</p>	<p>Potentially as good security as above, depending on applicant behavior. Allows applicant to specify code which is unique and private but unlikely to be lost (for example agent docket number).</p> <p>Also easy to deal with assignments and different rights-holders.</p> <p>Can be offered as an applicant option together with a basic access code system – unique code generated by OFF or IB if not specified by applicant.</p>	<p>Fractionally more complex than above for OFF.</p> <p>Slight risk of transcription error by OFF in addition to risks listed for basic access code system, above.</p>
<p><u>Managed access list using access control code</u></p> <p>(proposed system: list of authorized OSFs maintained by applicant on IB’s website, either on an individual or account basis)</p>	<p>Security at least as good as for access code for use by OSF (depending on applicant behavior) and potentially better since any codes defined by the applicant (and patterns of usage) are less likely to be revealed.</p> <p>Fewer burdens imposed on OSF in operating system.</p> <p>Fewer risks for applicant in transcribing codes accurately.</p>	<p>More complicated to develop IB system than access code (requires completely new system element for communicating with applicants).</p> <p>More complicated for applicant than basic access code system since requires further actions to specify Offices which should have access. This could be mitigated in an account-based system by allowing applicant to specify default Offices. Failure to set correct access in good time may negate rights at OSF.</p>
<p><u>“Unique object”</u></p> <p>(such as USB stick)</p>	<p>High security.</p>	<p>Very difficult to implement. Common systems needed at all participating Offices (OFF, OSF and probably IB).</p> <p>Depending on implementation, may require generation of multiple objects, little cheaper or easier than use of the p-docs themselves.</p>

<i>System</i>	<i>Pros</i>	<i>Cons</i>
<u>PKI system using smart cards or soft certificates</u>	High security. If well-implemented, could be easy for large filers going to automated Offices.	Requires common technology at OFF and OSF. Depending on implementation, might require applicant-Office systems development in addition to simply Office-Office communication protocol in every OSF. May require equivalent smart-card or certificate to be available for use by different agents acting before OFF and OSF. Applicant required to have special technology available, which may be difficult for applicants from developing countries or occasional filers.

Entry of priority documents into the DAS system; Allocation or confirmation of access control codes

13. The system will need to work with digital libraries held by Offices which act under different legal constraints in relation to the confidentiality of applications and applicant details. Certain bilateral priority document exchange systems have been difficult to use efficiently because of the need for the applicant to sign a complex confidentiality waiver in order for the application to be made available in that way. It is desired to avoid this difficulty, so it seems to be necessary to deal with three possible routes, illustrated in Figures 3, 4 and 5, below:

(a) Route A: The OFF holding the digital library is able to send to DAS both a reference to the priority document and some applicant contact information (either physical mailing address or e-mail address);

(b) Route B: The OFF is able to send to DAS a reference to the priority document, but no further details until the applicant approaches the DAS directly with an access control code which has been assigned; or

(c) Route C: The OFF is not able to send any information at all to DAS until the applicant gives DAS an access control code recognized by the OFF. Under this option, a confirmation of availability can only be provided to the applicant by DAS once availability has been confirmed with the OFF, implying delays in such feedback if DAS and the OFF in question do not have a dedicated real-time mechanism in place to support the confirmation.

14. The flows of data required are shown in Figures 3 to 5. In each case, the applicant will have an access control code sent (or confirmed, if one has already been specified by the applicant) either by the OFF or by DAS. Using Route A, DAS will be able to confirm to the applicant that the system has correctly recognized the priority document. Using Routes B and C, the confirmation may only be possible at a later time than under Route A, namely, when the applicant first submits the code to DAS to manage the access list since prior to that time, the system may have no record of the application, or else insufficient information to activate the access control code within DAS.

Security of delivery

15. The security of the system also requires that the identity of Offices offering digital libraries or attempting to access a priority document be confirmed. However, this does not require special consideration because, whereas the identity of a person claiming to be an applicant is difficult to verify, the Offices involved are a limited group with which the International Bureau already has trusted communication channels. Each of the systems which are proposed to be used for communications already includes a means for establishing a secure channel between the International Bureau and a point which can be identified as a particular Office.

Figure 3

**DAS Entry – Route A:
OFF releases p-doc reference and applicant details to DAS**

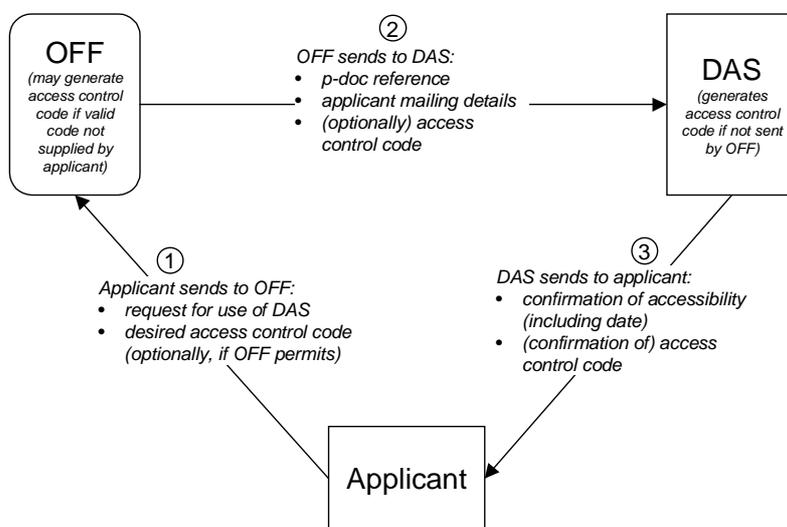


Figure 4

**DAS Entry – Route B:
OFF releases p-doc reference to DAS, but not applicant details**

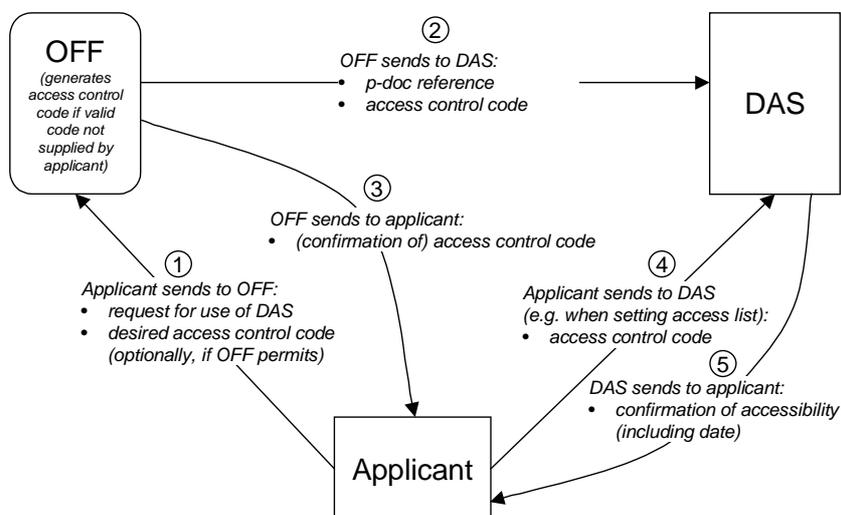
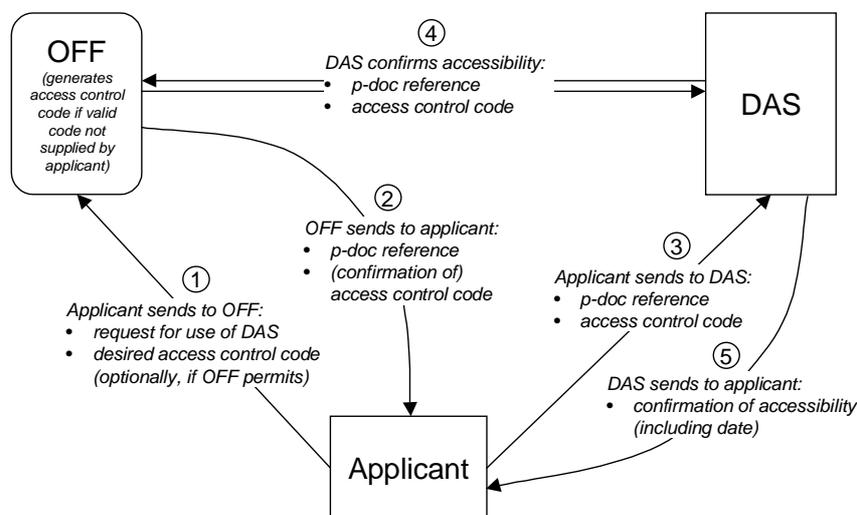


Figure 5

**DAS Entry – Route C:
OFF releases no details directly to DAS**



TECHNICAL CONSIDERATIONS

16. A number of technical considerations have arisen to complement or supersede those outlined in paragraph 22 of the system architecture document that was submitted to the Working Group at its first session (document WIPO/DAS/PD/WG/1/5). Technical considerations now include the following:

- (a) Initially, the system will only support black and white documents; color and gray-scale will not be supported.
- (b) The system needs to be able to handle withdrawal by the applicant of permission to distribute a priority document, although authorization of a particular OSF cannot be revoked by the applicant after a priority document has already been accessed by that OSF.
- (c) For reasons of both information security and legal certainty, the system needs to record the dates on which priority documents become available to the system, on which access permissions are set or removed, and on which Offices access, or attempt to access, a document.
- (d) Handling of translations of priority documents will be required as a future development.
- (e) While priority documents will be held for the purposes of DAS in digital libraries, the system must also support paper-based submission and distribution of priority documents, access list maintenance and requests for access, for the benefit of smaller Offices and applicants not possessing the necessary automated systems or internet access.
- (f) The system will need to handle lost or compromised access control codes.

(g) Consideration is needed of how the arrangements can properly handle changes in applicant information, such as address for correspondence, changes in ownership, deceased applicants, etc.

(h) Since authentication of access via the service relies on an access control code for each priority document, applicants must be made aware of the need to keep access control codes secure and to send them to other parties (such as in the case of changes of ownership) in a secure fashion, such as via normal mail.

(i) Requirements for access control codes need to be determined: for example, the allowable length and acceptable range of characters need to be defined.

(j) If requested data is bigger than MAXSIZE, physical media such as DVD should be sent instead of network transfer. MAXSIZE and transmission details need to be determined during the implementation phase.

(k) Online access list management may require a real-time request/response of accessibility to/from TDA or other digital libraries.

(l) The system should be able to decide which version of a document to select in case it is informed of the existence of versions held in different libraries. For example, a version held in a library maintained by the actual OFF might be preferred, but otherwise the first-notified certified copy from another digital library could be used.

(m) Details on the technical means by which DAS would recognize or be notified that a priority document is publicly available.

17. In addition to the technical considerations listed above, a more concrete definition of the handling of corrections to priority documents and (eventually) translations needs to be considered in order to define the requirements of the system. In particular, should Offices which have accessed a document be automatically informed of a corrected version?

18. In order to deliver a system quickly and at minimum cost, which is capable of offering as large a range of priority documents as possible to as large a range of Offices as possible, it is proposed that development work focus initially on providing communications using the TDA protocol (a generic document interchange standard used by the Japan Patent Office, the United States Patent and Trademark Office and the European Patent Office, but open to implementation by other Offices) and the systems currently in place for communication of PCT documents and information. Offices wishing to use the system would be encouraged to use one of these communication methods, but consideration could be given to adding further communications options, if necessary, once the basic system has been implemented.

19. *The Working Group is invited to:*

(i) *recommend that the digital access service system architecture be based on a managed access list system, as described in paragraphs 7 to 15, above;*

(ii) *agree that the means for addressing technical considerations set out in*

paragraph 16 should be determined by the International Bureau in the process of developing the system;

(iii) give advice on the system requirements referred to in paragraph 17, above; and

(iv) recommend that initial development work should focus on the use of TDA and PCT communication services as described in paragraph 18.

[Annex follows]

ANNEX

EXTRACT FROM THE REPORT OF THE
FIRST SESSION OF THE WORKING GROUP
(document WIPO/DAS/PD/WG/1/6, paragraphs 14 to 32)

SYSTEM ARCHITECTURE

14. Discussions were based on documents WIPO/DAS/PD/WG/1/2 and 5¹. The Secretariat explained that document WIPO/DAS/PD/WG/1/2, insofar as it described the proposed system architecture, had in effect been superseded by document WIPO/DAS/PD/WG/1/5.

15. In introducing the documents, the Secretariat emphasized the following points:

(a) The system architecture of the new service would need to be refined taking into account the considerations of the Working Group. The architecture as proposed offered at least the same levels of confidentiality and security as already applied under the Patent Cooperation Treaty (PCT). The proposed architecture would be complementary to other document exchange systems, in particular the Trilateral Document Access (TDA) system (see paragraph 16, below).

(b) The proposed system architecture was designed to be flexible, allow for a wide variety of the possible data flows between the applicant, the Office of first filing, the Office of second filing, and the International Bureau. The service would wherever possible take advantage of existing PCT infrastructure, including scanning facilities and the Electronic Data Interchange (PCT-EDI), Communication on Request (PCT-COR) and PatentScope systems.

(c) The proposed access system relied on use of an access code which could act as a substitute for a priority document itself, and would allow applicants to manage the distribution of a priority document without the need to handle it.

(d) Three particular issues related to the proposed system architecture that needed consideration were:

(i) *Means of delivery of priority documents to Offices of second filing:* A new secure part of the PatentScope web site might be used, allowing for browser-based access to the priority document. Alternatively, the PCT-EDI system, based on the Secure File Transfer Protocol (SFTP), might emerge as a better delivery mechanism, as it had an Office authentication mechanism, and could be used for simple bulk data delivery.

(ii) *Centralized versus decentralized management of the distribution of priority documents to Offices of second filing:* The proposed architecture foresaw the applicant transmitting an access code to each Office of second filing in a decentralized fashion. The Working Group might wish to consider the merits of a system permitting applicants to use an access code to enter a centralized system from which the distribution of priority documents to Offices of second filing could be managed.

¹ A footnote that appeared at this point in document WIPO/DAS/PD/WG/1/6 has been omitted.

(iii) *Whether the access code should be generated and sent to the applicant by the Office of first filing or the International Bureau:* Under the proposed architecture, the Office of first filing would transmit the mailing address of the applicant and other meta-data to the International Bureau, which would generate and transmit the access code to the applicant. Users of the system might find it more convenient for the access code to be generated and sent to the applicant by the Office of first filing.

16. The Delegation of the United States of America, speaking also on behalf of the Delegation of Japan and the European Patent Office, welcomed the initiative to establish a digital access service for priority documents. The Delegation noted that the three Offices concerned (the “Trilateral Offices”) held a substantial majority of the world’s priority documents, and had already established a Trilateral-based digital access service called Trilateral Document Access (TDA) to facilitate transfer of priority documents between those Offices. The Delegation further stated that the Trilateral Offices shared the following views: (i) Security and access to unpublished applications are critical issues that must be addressed before the service can be considered usable. (ii) Similar to the Trilateral arrangement, the service should be free of charge to users. (iii) Given the substantial investment by the Trilateral Offices in the development and implementation of TDA, it was imperative that the integrity of TDA be maintained and that it be controlled by the Trilateral Offices, and that as a result, the Trilateral Offices favored a network or distributed model of cooperating services. The Delegation’s comments are reproduced in the Annex².

Agreed Principles³

17. The Working Group, after considerable discussion, agreed that the digital access service for priority documents should be developed having regard to the following principles, noting that they might be subject to evolution with future consideration by the Working Group and that further principles might need to be included:

“1. Business need

- (i) The fundamental requirement is to allow applicants to meet priority document requirements of Offices of second filing without having to physically obtain and submit certified copies with each of them.
- (ii) The system will enable voluntary participation by Offices from any Paris Union Member State, regardless of membership of other Treaties, taking into account the different capacities of Offices.
- (iii) Offices will be able to choose to obtain priority documents under an arrangement with the International Bureau as an alternative to multiple bilateral arrangements.
- (iv) The system must provide performance improvements and efficiencies for applicants, Offices and the International Bureau over traditional Paris Convention and paper-based arrangements.

² The Annex to document WIPO/DAS/PD/WG/1/6 is not reproduced here.

³ A slightly modified text of the agreed principles is proposed for approval by the Working Group as set out in Annex II of document WIPO/DAS/PD/WG/2/3.

“2. *Network model*

- (i) *Non-duplication of systems:* The system will make use of digital libraries in which Offices hold priority documents. The International Bureau’s digital library will hold priority documents from Offices which do not maintain their own.
- (ii) *Interoperability:* Common protocols and meta-information will be used to ensure that priority documents can be accessed in the same manner irrespective of the digital library in which they are held, be it the International Bureau’s, under TDA, or another.

[Diagram⁴]

- “3. *Flexibility:* The system will allow a wide range of combinations of packaging channels (including paper, physical media (CD-R and DVD), SFTP and TDA) and document format (including paper, ST.36, PCT minimal specification (based on PDF and TIFF) and SDIF) in order to ensure that all existing systems for exchanging priority documents are accommodated. The system will permit the transformation of format in order to facilitate interoperability.
- “4. *Secure data transmissions:* The security of data transmissions will be at least equivalent to the levels that apply in the systems operating in the context of the PCT for the exchange of sensitive data.
- “5. *Confidentiality:* There must be an appropriate mechanism, in relation to priority documents that are not publicly available, for ensuring that access is given to Offices of second filing only where authorized by the applicant. One possible mechanism would rely on the use of an access code issued to the applicant, but other possible mechanisms need to be explored and evaluated so as to achieve minimum burden for Offices and applicants.
- “6. *Translations and other documents:* The system will enable applicants to deposit certified translations of priority documents in a digital library for making them accessible to Offices of second filing under generally similar arrangements to those for priority documents. Further work is needed to address the implications of different Offices’ certification requirements for translations, the possibility of obtaining translations from other sources, and the possible use of the system for other associated documents, for example, documents confirming the right of priority, in particular where the right is transferred to other persons.

⁴ A conceptual diagram of a networked system illustrating access by an Office of second filing that appeared at this point in document WIPO/DAS/PD/WG/1/6 appears as Figure 1 in the main body of the present document and has therefore been omitted here.

“7. *Efficiency*

- (i) *Avoid duplication:* Duplication of work, data holdings and information between the International Bureau and Offices will be avoided. This applies in particular to existing digital libraries such as under TDA arrangements.
- (ii) *Improve technical capacity:* The system will be geared to handle large volumes of data and data transmissions, with appropriate speed of uploading and downloading, with built-in flexibility to cater to potentially increased needs in the future.
- (iii) *Transparency:* WIPO’s website will provide up-to date details about the system, including the conceptual framework, the nature and scope of participation by Offices in the system, the location of priority document holdings, Office requirements and operational details, including changes in those things.

“8. *Developing countries:* The International Bureau will provide technical assistance and adequate capacity building to developing countries, in particular least developed countries, based on discussion of their individual needs, to facilitate their participation in the system.

“9. *Charges:* The International Bureau will not charge a fee for use of the service.”

18. The Delegation of the United States of America reserved its position as to the possible use of the new service for making available documents relating to assignments of rights (see item 6 in the agreed principles set out in paragraph 17, above).

19. Certain other matters on which comments or clarifications were made during the discussions, apart from matters encapsulated in the agreed principles set out in paragraph 17, above, are noted in summary form in the following paragraphs.

20. *Contents of digital libraries:* It was confirmed that the digital access service would allow Offices to retrieve the full priority documents from the digital libraries, not only bibliographic details. The priority documents themselves would, of course, be in their original languages. The system would need to handle translations eventually, even if this was not part of the initial system. However, further consideration was needed of the best way to treat them, noting that they were not documents of record in the same way as the original documents.

21. *Certification:* It was clarified that it was envisaged that both priority documents and translations loaded into digital libraries under the new service would be available. When access to a priority document was obtained under the service by an Office of second filing, the Office would be obtaining a copy of the certified original, the validity of the copy being assured by the fact that it had been obtained under the service administered by the International Bureau. In that respect, the procedure would be the same as that which had long operated successfully under the PCT in relation to priority documents. The available procedures for certification of priority documents (as distinct from translations, for which different requirements applied) should be understood in accordance with the agreed understanding adopted in 2004 by the Assemblies of the Paris Union and the PCT Union (reproduced in Part E of the Annex to document WIPO/DAS/PD/WG/1/2).

22. *Submission direct by applicants:* It was noted that further consideration was needed of what procedures should apply when priority documents and translations thereof were submitted direct by applicants for uploading into a digital library under the service.

23. *Period of availability of documents via the service:* It was noted that priority documents may be needed after the grant of a patent, and the service should accordingly provide for access for at least as long as the term of the relevant patents claiming priority. It needed to be recognized that, particularly in a distributed system such as was proposed, long-term availability of documents could not be absolutely guaranteed, and provision needed to be made to govern what could be done if a particular document ceased to be available. Offices of second filing would always be entitled, in such cases, to request the applicant to provide it, but applicants should not be penalized if they had complied with the requirements for making documents available via the service.

24. *Priority documents becoming publicly available:* It was noted that authorization of access by an Office of second filing should not be needed after a priority document had become publicly available (see also paragraph 38, below⁵). The question whether third parties should have access via the service to publicly available priority documents needed further consideration, as did the ways in which a priority document might become publicly available.

25. *System capacity:* In response to concerns expressed about the speed of access to certain PCT services on which the system might be based, the Secretariat explained that this was not an issue of capacity of PCT systems themselves, but of limitations on Internet bandwidth between certain parts of the world. Nevertheless, the International Bureau was investigating possible arrangements with a third party Internet distribution supplier to improve data delivery to affected regions.

26. *Technical assistance and capacity building:* The Secretariat explained that WIPO's program for Office automation assistance had significantly evolved over the past few years. The Industrial Property Automation System (IPAS) common software, which automated the business processes of industrial property Offices, was provided to Offices free of cost, together with technical and financial assistance for its deployment. At present this software was being used by about 35 Offices. It was regularly maintained by way of updates and additional modules to extend its functionalities. The software was being migrated to the Java platform, which would allow its use through a web browser and provide greater flexibility for further enhancements. The deployment methodology was continually being refined, and WIPO provided post-deployment assistance and training to Offices. WIPO had also developed a methodology for assisting Offices in digitizing their records and, as a result, in developing comprehensive databases.

27. *Changes in national laws and regulations:* It was noted that certain aspects of the operation of the new service may need to be implemented by changes in national laws (in particular, the need for recognition of priority documents obtained via the service for the purpose of meeting Paris Convention requirements in relation to priority documents). It seemed likely that such changes would be needed to regulations rather than the parent patent

⁵ Paragraph 38 of document WIPO/DAS/PD/WG/1/6 is not reproduced here but is reproduced in document WIPO/DAS/PD/WG/2/3.

laws. The Secretariat confirmed its preparedness to provide advice and assistance in this respect to Offices which so requested.

Technical breakout sessions

28. Informal breakout sessions, in which all delegations were invited to participate, were held with the aim of considering some of the technical issues involved in the new service. At the invitation of the Chair, the Delegation of Canada outlined to the Working Group the main points that had been discussed in the first breakout session. The discussions had centered on two main components, namely, flow of data and control of access by Offices of second filing.

29. In relation to *flow of data*, the breakout session had identified a number of scenarios which needed to be considered, including the following:

(i) where the Offices of first and second filing were both part of a system covered by a different bilateral or multilateral agreement, such as TDA, in which case WIPO's digital access service would not need to be used, although its use would not be excluded;

(ii) where the Office of first filing communicated electronically with the International Bureau and maintained its own digital library;

(iii) where the Office of first filing communicated electronically with the International Bureau and did not maintain its own digital library;

(iv) where the Office of first filing did not communicate electronically with the International Bureau and paper documents needed to be sent;

(v) where the applicant wished to submit translations to the system; and

(vi) where it was desired to make corrections of errors in priority documents and notify the corrections to Offices of second filing which had already accessed the incorrect version (for example, if it was found that a page had been missed when the document was scanned by the Office of first filing or the International Bureau).

30. In relation to *access control*, the breakout session had considered various options covering ways in which the applicant might specify which Offices were permitted to access the priority document. Most of the discussion had focussed on a system under which the International Bureau issued a code to the applicant. Further possibilities were identified for the use of such a code, beyond that outlined in document WIPO/DAS/PD/WG/1/5 whereby the applicant would provide the code to Offices of second filing for use in requesting access. One such possibility was that the applicant could use it to access information about the status of the priority document within the system. Another possibility was for use of the code by the applicant to establish and maintain a list of those Offices of second filing that were permitted to access the priority document, in which case the list would be used by the service as a means of validating requests for access by Offices of second filing, the applicant would be relieved of the need to quote the code with each later filing, and Offices of second filing would not need to store or use the code to gain access.

31. Diagrams illustrating the data flow scenarios and further possibilities for use of the code, as outlined in paragraphs 29 and 30, above, were made available to delegations and would be posted on the priority documents electronic forum on WIPO's website.

32. The Chair noted that those present at the breakout sessions had found them very useful, and suggested that they take place again at the Working Group's next session in order to better prepare the matters discussed for consideration by the Working Group, although of course it remained a matter for the Working Group to agree on a recommended system architecture. Delegations were encouraged to participate in further consideration of the matters via the electronic forum.

[End of Annex and of document]