Proposed Amendments to both the .eu ADR Rules
&
Supplemental Rules

1. Proposed Amendments to .eu ADR Rules

Class Complaint

- The following new definition is to be added in Par. A1 of the ADR Rules:

"Class Complaint" means a single Complaint filed against a single domain-name holder in regard to multiple disputed domain names with the same language of proceeding filed by a single person acting on behalf of two or more Complainants and requesting separate relief for each Complainant for different disputed domain names than for the other Complainants joined in the Class Complaint."

- Par. A4 (c) of the ADR Rules is to be modified as follows:

"(c) The *Panel* shall terminate the *ADR Proceeding* if it becomes aware that the dispute that is subject of the *Complaint* has been finally decided by a court of competent jurisdiction or an alternative dispute resolution body. Notwithstanding anything mentioned in this Par. A4 (c), in case a *Class Complaint* is rejected in an *ADR Proceeding* pursuant *to ADR Rules*, each of the *Complainants* joined in the *Class Complaint* can file individual *Complaint(s)* with respect to the disputed domain names included in the rejected *Class Complaint*."

- Par. B1 (c) of the ADR Rules is to be modified as follows:

"(c) The *Complaint* may relate to more than one domain name, provided that the *Parties* and the language of the *ADR Proceedings* are the same or the *Complaint* is in the form of a *Class Complaint*."

- New Par. B1(d) is to be inserted in the ADR Rules with the following wording:

"(d) It is possible to file a *Class Complaint* provided the following conditions are met:

- The Class Complaint is based on legal arguments applicable equally, or substantially in the same manner, to all the disputed domain names;
- the person representing several different Complainants joined in the Class Complaint must provide evidence that it is authorized to act on behalf of each of the Complainants; and
- for the avoidance of doubt, the Panel can order transfer of any of the disputed domain name(s) only to the individual Complainant on which behalf such transfer was requested in the Class Complaint, in accordance with the ADR Rules and ADR Supplemental Rules."

Electronic-only ADR

- The following new definition is to be added in Par. A1 of the ADR Rules:

"*Secure Authentication* means a method of authenticating electronic communications and/or documents filed in electronic form via the on-line platform of the Provider. It is a secure process which not only establishes the identity of the Party (or its authorized representative) communicating and/or filing documents via the Provider's on-line platform but also provides strong evidence that the integrity of the communications or documents sent has been preserved and that the Party approves of and intends to be bound by its contents."

- New Pars. for A3 are to be inserted in the ADR Rules with the following wording:

"3 Electronic-only ADR Proceeding

(a) Filing an electronic-only *Complaint* or *Response* is possible, provided that the *Party* making the electronic-only submission uses *Secure Authentication* in accordance with detailed conditions specified in the *ADR Supplemental Rules*.

(b) As to an electronic-only *Complaint* or *Response*, the signature of the *Complainant* or *Respondent* (or that of their authorized representatives) can be in the form of a data message complying with the detailed conditions found in the *ADR Supplemental Rules.*

(c) When electronic-only submissions are filed pursuant to Par. A3, the *Provider* will identify them as "electronic-only" in the case file of the *Provider*'s on-line platform.

(d) If a *Party* files electronic-only submissions pursuant to Par. A3, the *Provider* will be responsible for printing the submissions and mailing them to the other *Party* provided that it is obliged to satisfy the obligation given in Par. A2(b) and/or A2(c)(3) of the *ADR Rules*, requiring hardcopies of documents to be mailed to the other *Party*.

- Par. B1 (b) of the ADR Rules is to be modified as follows:

"(b) Unless a *Complaint* is submitted in electronic form only (and it complies with Par. A3 above), the *Complaint* shall be submitted in hard copy and in electronic form , and it shall: …"

- Par. B3 (b) of the ADR Rules is to be modified as follows:

"(b) Unless a *Response* is submitted in electronic form only (and it complies with Par. A3 above), The *Response* shall be submitted in hard copy and in electronic form, and it shall: …"

2. Proposed Amendments to the .eu ADR Supplemental Rules

Electronic-only ADR

- Par. A5 of the ADR Supplemental Rules is to be modified as follows:

"5 Electronic-only ADR

For the purposes of .eu ADR, either of the two following concepts is considered as producing *Secure Authentication*, as defined in the *ADR Rules*:

(a) Using advanced electronic signatures based on qualified certificates as defined in Directive 1999/93/EC on a Community framework for electronic signatures; or
(b) Employing the Strong Authentication process described in Annex D of the ADR Supplemental Rules."

- New Annex D is inserted:

"Annex D: Specification of Strong Authentication process"

[See below]

Annex D: Specification of Strong Authentication process

Concept
Strong Authentication

The following is a specification of the Strong Authentication process.

Strong Authentication (of two factors)

A two-factor method of Strong Authentication will be applied. The two factors are 1) the knowledge of a password (something known, the single factor) and 2) providing the correct answer to a question (which is possible to do only when possessing a shared secret– the grid or "BINGO Card," the second factor).

This allows for a good balance between security and usability.

An example of the grid is shown below:

.eu ADR	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	9	4	6	4	1	8	4	1	4	7	4	7	9
2	7	1	6	8	5	0	0	3	6	8	5	1	9	8
3	9	5	8	7	3	2	1	2	7	2	3	6	3	5
4	1	7	9	0	2	6	4	7	9	1	5	2	4	1
5	5	2	6	5	9	7	3	0	8	3	2	8	3	6

The format of the grid (or BINGO Card) is very flexible. Its contents could be numeric, alphanumeric, etc. What is important is that each user has a unique, randomly generated grid that he will use for the second factor of authentication.

The authentication question is associated with the specific user account, based on the first step of authentication – username and password.

In the example above, the user is called upon by the on-line platform to supply the correct answer using certain grid coordinates—for example B5, C3, M4, D3 and G1. The user would respond with the grid cell contents that correspond to the coordinates asked. In this example, the user would enter the grid locations for location
B5, C3, M4, D3 and G1. - "2", "8", "4", "7", and "8." For each subsequent login, a different random quiz would be generated and the user would be prompted for the appropriate response. Thus, the user has a second factor for authentication with a one-time challenge and response mechanism, designed to be resistant to fraudulent impersonation.

The application of the Strong Authentication method contains other process mechanisms safeguarding the security of the system.

Namely:

1. A trustworthy handover of the BINGO Card and the initialization password. An interested Party will receive his username when registering on-line. Then, his BINGO Card and initialization password will be sent separately (by registered mail or express courier, with confirmation of delivery) to the addresses he indicated during his on-line registration.

2. Once the Party logs in for the first time, his card is initialized. Then, he requests a password for further logins, using Strong Authentication; the new login password is sent to him via the on-line platform.

3. It is possible to change a Party's data (including the login password) only after Strong Authentication; the new login password is sent to him via the on-line platform.

4. The card will have an expiration date after which it is no longer valid.

5. If the card is lost or damaged, or if there is the suspicion that it has been or will be copied, the Party is obligated to inform the CAC of the matter immediately, whereupon the card is blocked and a new card will be sent to him. Access to the account will be possible only after initializing the new card.

Supplemental Processes

Under the Strong Authentication process, additional measures will be implemented helping to ensure all the properties demanded for Secure Authentication.

1) Familiarization/request
The Party is demonstrably familiarized with the whole process of Strong Authentication and the conditions of its application. Please see the on-line presentation of the Strong Authentication process and its individual steps at www. adr.eu/_____

2.) Acceptance (INTEGRITY)

The documents filed electronically through the Strong Authentication will be posted on the on-line platform, together with their hash function. The receipt by the CAC of every document filed by a Party using Strong Authentication will be automatically acknowledged by e-mail (*i.e.*, a communication channel other than the on-line platform), requesting the Party to check his documents stored on the on-line platform and to confirm, using Strong Authentication through the on-line platform, whether:

- the documents stored conforms fully with those he submitted (verification of integrity);
- he approves of the contents of the document; and
- he intends to be bound by the document.

If the Party does not submit his verification within 48 hours of notification, the electronic submission will be considered as withdrawn and nullified.

3) SSL Communication
(IDENTIFICATION + IRRECUSABLE OPERATION + CONFIDENCE)

After the Party logs in to the on-line platform (in accordance with the steps described above), all communication will take place with the aid of SSL.