DEFECT REPORT FORM

1. Defect Report Number: 202

   Title: Clarification of **CertificationPath** in **SecurityParameters**

2. Source: Defect Resolution Group

3. Addressed to: ISO/IEC JTC1/SC6/WG7 and ITU-T SG VII Editor Group on the Directory

4. (a) WG Secretariat: UK (BSI)
   (b) ITU-T WP: WP 4

5. Date Circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning:
   (number and title of IS or DIS final text/CCITT Recommendation)

   ITU-Rec. X.511 | ISO/IEC 9594-3

8. Qualifier: (e.g.: error, omission, clarification required)

   clarification

9. References in Document: (e.g.: page, clause/section, figure, and/or table numbers)

   clause 7.10

10. Nature of Defect: (complete, concise explanation of the perceived problem)

The paragraph describing **CertificationPath** does not make it clear that the sender's user certificate is present. Also the use of term "certificate pairs" can cause confusion. The certificate pair attribute may be held in the Directory but only one of the pair would be used in the protocol. The certificate may be that of a CA or a cross certificate. Rather than explaining all this, the text should be simplified and a reference to the Authentication Framework inserted.

The paragraph describing **time** states that it is the expiry time of the token; the token is used in a bind and there is a specific definition of **time** used in a token. In security parameters **time** should specify an expiry time for the request argument, response, or error.

The paragraphs describing **random** again mentions token. Like **time**, **random** is for a request argument, response, or error.

The text states that **time** and **random** are only used when the request argument, response, or error is signed. These security parameter components can be used in an unsigned request argument, response, or error. Although signing does provide integrity and data origin authentication, there are other methods, e.g. a VPN.

11. Solution Proposed by the Source: (optional)

Note that the following DTC text is proposed for the 3rd edition. Remove references to signed errors to generate text for the 2nd edition.

Replace the paragraph describing ***CertificationPath*** *with the following*

The **CertificationPath** component is a sequence containing the signer's user certificate, and, optionally, a sequence of one or more certification authority (CA) certificates. (See clause 8 in ITU-T Rec. X.509 | ISO/IEC 9594-8). The user certificate is used to bind the signer's public key and distinguished name, and may be used to verify the signature on a request argument, response, or error. This parameter shall be present and contain the signer's user certificate if the request argument, response, or error is signed. Additional certificates may be present and may be used to determine if the signer's user certificate is valid. Additional certificates are not required if the recipient shares the same certification authority as the signer. If the recipient requires a certification path for validation, and an acceptable parameter is not present, whether the recipient rejects the signature, or attempts to determine a certification path, is a local matter.

Replace the paragraph describing ***time*** *with the following*

The **time** is the intended expiry time for the validity of the request, response, or error. It is used in conjunction with the random number to enable the detection of replay attacks.

Replace the 1st paragraph describing ***random*** *with the following*

The **random** number is a number that should be different for each request, response, or error. It is used in conjunction with the time parameter to enable the detection of replay attacks. If sequence integrity is required then the random argument may be used to carry a sequence integrity number as follows:

12. Editor's Response:

Accepted at Orlando 99