

**CONGRUENT SOFTWARE, INC.**  
**3998 Whittle Avenue**  
**Oakland, CA 94602**  
**(510) 531-5472**  
**(510) 531-2942 FAX**

FROM: Peter Johansson  
 TO: T10 SBP-2 *ad hoc* Working Group  
 DATE: September 16, 1997  
 RE: Proposed SBP-2 Annex for Security

---

As a consequence to the directions agreed in the joint disk boys, SBP-2 and SCSI meeting Wednesday, September 10, in Nashua, I propose that the security model be added to SBP-2 as an optional feature. Most of the model is contained in a new normative annex for SBP-2; changes required in other, stabilized portions of the document as well.

I propose that Table 2 in 5.1.4, "Management ORB's," be modified as shown below:

**Table 1 – Management request functions**

Value	Management function
0	LOGIN
1	QUERY LOGINS
2	CREATE STREAM
3	RECONNECT
4	<a href="#">SET PASSWORD</a>
5 – 6	Reserved for future standardization
7	LOGOUT
8 – 9	Reserved for future standardization
A <sub>16</sub>	TERMINATE TASK
B <sub>16</sub>	ABORT TASK
C <sub>16</sub>	ABORT TASK SET
D <sub>16</sub>	CLEAR TASK SET
E <sub>16</sub>	LOGICAL UNIT RESET
F <sub>16</sub>	TARGET RESET

The remainder of this document is the proposed normative annex for SBP-2. Although labeled annex X, I suggest that it become annex C when added to the draft.

## Annex X (normative)

### Security extensions

SBP-2 specifies an access protocol, in section 8, that by itself makes no provisions for security. This annex defines extensions to SBP-2 that may be implemented by targets to provide some measure of security. Targets that implement these security extensions shall conform to all provisions of this annex.

Conformance to this annex does not preclude additional, command set-dependent security facilities.

#### X.1 Passwords

A target shall implement two passwords:

- The master password, which shall be unchangeable and equal to the target serial number. The target serial number should be in a humanly readable form affixed to the target. The master password shall not be readable *via* the target's Serial Bus interface except by a logged-in initiator; and
- The current password, which may be changeable. If the current password is changeable, it shall accommodate 28 bytes of password data and shall not be alterable except by the set password function (see X.3).

All password values shall be unchanged by power reset, bus reset or command reset.

The value of the master password shall be obtainable by command set-dependent means.

A target may be manufactured with a current password of all zeros, with the expectation that the user assign a nonzero current password as part of target initialization. If a target is manufactured with a nonzero current password, the target shall be shipped with the current password in a humanly readable form.

#### X.2 Login

The description of the login protocol below reproduces that specified by section 8 and adds a validation of the *password* field from the login request. The target shall perform the following to process a login request:

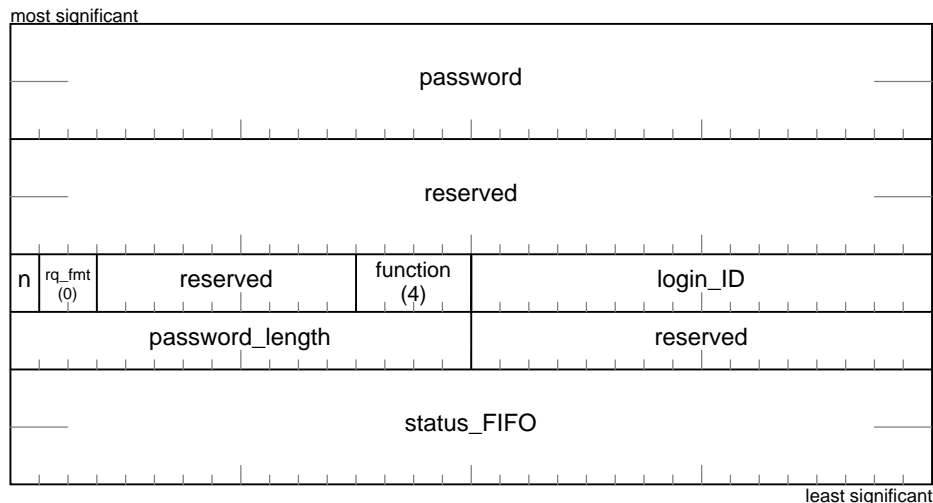
- a) The target shall read the initiator's unique ID, EUI-64, from the bus information block by means of two quadlet read transactions. The *source\_ID* from the write transaction used to signal the login ORB to the target's MANAGEMENT\_AGENT register shall be used as the *destination\_ID* in the quadlet read transactions;
- b) The target shall determine whether or not the initiator already owns a login by comparing the EUI-64 just obtained against the *login\_owner\_EUI\_64* for all *login\_descriptors*. If the initiator is currently logged-in to the same logical unit, the login request shall be rejected;
- c) The target shall validate the password provided by the login request. If *password\_length* is zero, the password is eight bytes of immediate data present in the *password* field. Otherwise *password\_length* specifies the size of the password addressed by *password*. In either case, the password value provided is extended to 28 bytes by adding least significant bytes of zeros and the result is compared against the target's password(s). If the password provided fails to match either the target's current or master password, the login request shall be rejected;

- d) If the *exclusive* bit is set in the login ORB, the target shall reject the login request if there are any active *login\_descriptors* for the logical unit;
- e) If an active *login\_descriptor* with the *exclusive* attribute exists for the *lun* specified in the login ORB, the target shall reject the login request; and
- f) The target shall determine if a free *login\_descriptor* is available. If a *login\_descriptor* is free, the initiator's *source\_ID* is stored in *login\_owner\_ID*, the initiator's EUI-64 is stored in *login\_owner\_EUI\_64*, the *lun* from the login ORB is stored in the *login\_descriptor*, the *exclusive* variable in the *login\_descriptor* is set to the value of the *exclusive* bit from the login ORB and the addresses of the fetch agent(s) are also stored in the *login\_descriptor*. Lastly the target assigns a unique *login\_ID* to this login and stores it in the *login\_descriptor*.

If the target is able to satisfy the login request, it shall return a login response as specified in 5.1.4.1.

### X.3 Set password

In order to change a target's current password, an initiator may use a management ORB with the format shown below.



**Figure X.1 – Set password ORB**

The *password* and *password\_length* fields specify the new value for the current password. If *password\_length* is zero, the *password* field contains immediate data. When *password\_length* is nonzero, the *password* field shall conform to the format for address pointers specified by Figure 11 and shall specify the address of a buffer. The maximum value of *password\_length* shall be 28. The buffer shall be in the same node as the initiator and shall be accessible to a Serial Bus block read request with a data transfer length less than or equal to *password\_length*.

The *notify* bit and the *rq\_fmt* and the *function* fields are as previously defined for management ORB formats.

The *login\_ID* field shall specify a login ID value obtained as the result of a successful login.

The *status\_FIFO* field shall specify an address allocated for the return of status for the SET PASSWORD request, only. The contents of this field shall not update the status FIFO address established by the successful login that returned *login\_ID*.

If *login\_ID* specifies a valid current login for the initiator that signaled the SET PASSWORD request to the target's MANAGEMENT\_AGENT register, the target shall update the current password to the new value specified by the set password request. The target shall not return completion status for the request unless either the request is rejected or the new password has been successfully stored such that it will not be affected by any subsequent power reset, bus reset or command reset.