Security guidelines for S@T Push

Copyright © 2019 SIMalliance ltd.

August 2019
The SIMAlliance recommends to implement security for S@T push messages. This security can be introduced at two different levels:

1. At the network level, filtering can be implemented to intercept and block the illegitimate binary SMS messages.

2. At the SIM card level, the Minimum Security Level - MSL - attached to the S@T browser in push mode can force Cryptographic Checksum + Encryption (MSL = 0x06 at least)

   In such cases where the replay of legitimate messages could lead to undesirable effects, MSL with Cryptographic Checksum + Encryption and anti-replay Counter is recommended (e.g. 0x16)