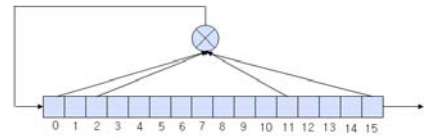


Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

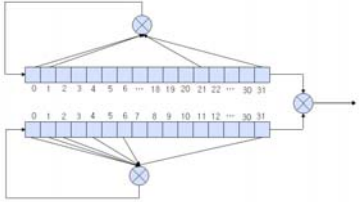
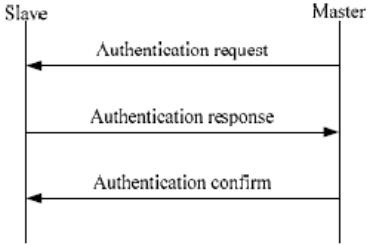
| | |
|--|--|
| Document Number: | N14030 |
| Date: | 2009-06-16 |
| Replaces: | |
| Document Type: | Disposition of Comments |
| Document Title: | Disposition of Comments on 6N13871, China's Comments on 6N13773 Text for CD ballot, ISO/IEC CD 29157 PHY/MAC specifications for short-range wireless low-rate applications in ISM band |
| Document Source: | Project Editor |
| Project Number: | |
| Document Status: | For your information. |
| Action ID: | FYI |
| Due Date: | |
| No. of Pages: | 6 |
| ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS) Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ; Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr | |

| 1 | 2 | (3) | 4 | 5 | (6) | (7) |
|-----------------|--|---|---|--|--|---|
| MB ¹ | Clause No./ Subclause No./ Annex (e.g. 3.1) | Paragraph/ Figure/Table/ Note (e.g. Table 1) | Type of com- ment ² | Comment (justification for change) by the MB | Proposed change by the MB | PE's Proposal |
| CN1 | Clause 4 | | ed | All acronyms used in this document should be contained in Clause 4 (Abbreviated terms). | For example, RF, GFSK and FSK are not in the abbreviations list. | Accepted |
| CN2 | 8.3 | | te | A message's data integrity and authenticity should be protected. | There should be a MIC (Message Integrity Code) field in the frame structure. The MIC value protects both a message's data integrity as well as its authenticity, by allowing verifiers to detect any changes to the message content. | The proposed CD incorporates the CRC (cyclic redundancy check) code for data integrity. It also uses group codes and security codes for authenticity. For more elaborate integrity and authenticity, we suggest implementing on higher layers. |
| CN3 | 9.3.2 | | ge | Detailed descriptions of security mechanism needed. For example, how does the device obtain the key which used in encryption and decryption processes? How are the message field data encrypted with security codes and how to decrypt it? | | <p>Encryption and decryption are performed through scan codes, security codes, and group codes which are known only to the communicating peer(s).</p> <p>Scan codes are used for synchronisation, and security and group codes for message encryption and decryption.</p> <p>16-bit maximal sequences are used for security codes and 32-bit Gold codes are used for group codes. The code generators are shown below.</p>  <p style="text-align: center;">Security Code Generator</p> |

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

| 1 | 2 | (3) | 4 | 5 | (6) | (7) |
|-----------------|--|---|---|---|--|--|
| MB ¹ | Clause No./ Subclause No./ Annex (e.g. 3.1) | Paragraph/ Figure/Table/ Note (e.g. Table 1) | Type of com- ment ² | Comment (justification for change) by the MB | Proposed change by the MB | PE's Proposal |
| | | | | | |  <p>Group Code Generator</p> |
| CN4 | 9.3.2 | | te | <p>According to the draft standard, communications are possible only when the scan codes of the receiver and the transmitter are identical. There should be a better authentication mechanism before communication.</p> | <p>For example, the authentication mechanism can use a pre-shared key which shall be held by both devices to authenticate the identity of each other and to establish the other keys, such as Security code, for protecting certain frames exchange.</p> <p>The basic processes can be proposed as follows:</p>  <ol style="list-style-type: none"> 1. A Master sends a Authentication request message including a Master Nonce to a Slave to perform the mutual authentication 2. When the Slave receives the Authentication request message from the Master: <ol style="list-style-type: none"> a) Generate a Slave Nonce b) Compute MIC Key Data field Encryption Key = f(pre-shared key, Slave MAC | <p>Scan codes are used only for synchronisation purposes. It is true that the communication is possible only when the scan codes of the receiver and the transmitter are identical, but it is not intended for authentication. More elaborate authentication measures may be incorporated in the upper layers if needed.</p> |

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

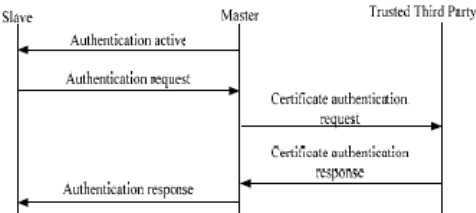
NOTE Columns 1, 2, 4, 5 are compulsory.

| 1 | 2 | (3) | 4 | 5 | (6) | (7) |
|-----------------|--|---|---|--|---|---------------|
| MB ¹ | Clause No./ Subclause No./ Annex (e.g. 3.1) | Paragraph/ Figure/Table/ Note (e.g. Table 1) | Type of com- ment ² | Comment (justification for change) by the MB | Proposed change by the MB | PE's Proposal |
| | | | | | <p>address Master MAC address Slave Nonce Master Nonce Other element)</p> <p>c) Compute Message Integrity Code using the MIC Key</p> <p>d) Send the Authentication response message including Slave and Master Nonce and Message Integrity Code to the Master</p> <p>3. When the Master receives the Authentication response message from the Slave:</p> <p>a) Check the validity of Master Nonce</p> <p>b) Compute MIC Key Data field Encryption Key = f (pre-shared key, Slave MAC address Master MAC address Slave Nonce Master Nonce Other element)</p> <p>c) Compute Message Integrity Code using the MIC Key</p> <p>d) Check the validity of Message Integrity Code</p> <p>e) Send the Authentication confirm message including Slave Nonce and Message Integrity Code to the Slave</p> <p>4. When the Slave receives the Authentication confirm message from the Master:</p> <p>a) Check the validity of Slave Nonce</p> <p>b) Check the validity of Message Integrity Code using the MIC Key</p> <p>In some cases, the authentication mechanism can also use a Certificate which can be identified by a trusted third party to achieve a peer mutual authenticate and to establish the other keys, such as Security code, for protecting certain frames exchange.</p> <p>The basic processes can be proposed as follows:</p> | |

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

| 1 | 2 | (3) | 4 | 5 | (6) | (7) |
|-----------------|--|---|---|--|---|---------------|
| MB ¹ | Clause No./ Subclause No./ Annex (e.g. 3.1) | Paragraph/ Figure/Table/ Note (e.g. Table 1) | Type of com- ment ² | Comment (justification for change) by the MB | Proposed change by the MB | PE's Proposal |
| | | | | |  <pre> sequenceDiagram participant Slave participant Master participant TTP as Trusted Third Party Master->>Slave: Authentication active Slave->>Master: Authentication request Master->>TTP: Certificate authentication request TTP->>Master: Certificate authentication response Master->>Slave: Authentication response </pre> <ol style="list-style-type: none"> 1. A Master sends a Authentication active message to perform the peer mutual authentication 2. When the Slave receives the Authentication active message from the Master, it send the Authentication request message including Slave Certificate, other element and its Signature to the Master 3. When the Master receives the Authentication request message from the Slave, it send the Certificate authentication request message including Master and Slave Certificate, other element and Master and Slave Signature to the trusted third party 4. When the trusted third party receives the Certificate authentication request message from the Master: <ol style="list-style-type: none"> a) Check the validity of two Signatures b) Check the validity of Slave and Master Certificate c) Sign Signature of the trusted third party to the result of the Slave Certificate verification d) Sign Signature of the trusted third party to the result of the Master Certificate verification e) Send the Certificate authentication response message including the results of | |

¹ **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

| 1 | 2 | (3) | 4 | 5 | (6) | (7) |
|-----------------|--|---|---|--|--|---------------|
| MB ¹ | Clause No./ Subclause No./ Annex (e.g. 3.1) | Paragraph/ Figure/Table/ Note (e.g. Table 1) | Type of com- ment ² | Comment (justification for change) by the MB | Proposed change by the MB | PE's Proposal |
| | | | | | <p>the Master and Slave Certificate verification, two Signatures of the trusted third party to the results and other element to the Master</p> <p>5. When the Master receives the Certificate authentication response message from the trusted third party:</p> <p>a) Check the validity of Authentication request message and slave identity</p> <p>b) Send the Authentication response message which is the same as the Certificate authentication response message to the Slave</p> <p>6. When the Slave receives the Authentication response message from the Master, it checks the validity of Master identity.</p> <p>7. Use "Other element" to establish the other keys, such as Security code, for protecting certain frames exchange.</p> | |

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.