



This declaration and all references to Certicom's Intellectual Property and licensing terms are Confidential information, per Clause 6 of the ZigBee Alliance Participation Agreement, and must be treated as such.

This information shall not be distributed outside the ZigBee Board of Directors, per Exhibit 2, Clause 3 (b) of the ZigBee Alliance Participation Agreement.

A. ZIGBEE ADOPTED SPECIFICATION or ZIGBEE PROPOSED SPECIFICATION:

Number: v0.92 ZigBee Specification Documents (as documented in Zipped file 2004-07-29_ZigBee_v0.92_Releases)

Title: ZigBee Alliance Security Services Specification, Revision 12, July 29, 2004 (document number: 03/322r12ZB)

B. MEMBER ORGANIZATION:

Legal Name of Member Organization: Certicom Corporation

If the Member is completing this Declaration to disclose Necessary Claims of an Affiliate or Non-Member, the Member must provide the following information:

Legal Name of Affiliate or Non-Member (check one): _____

Member is authorized to act on behalf of Affiliate or Non-Member (check one): Yes or No

C. CONTACT FOR LICENSE TERMS AND CONDITIONS:

Name of Organization: Certicom Corporation

Name of Individual & Department: Paul Carter, Intellectual Property Group

Address: 1800 Alexander Bell Drive, Suite 400, Reston, VA, 20191, USA

Telephone: +1 (703) 234-2357, ext 112 Fax: +1 (703) 234-2356 E-mail: pcarter@certicom.com

D. POSITION REGARDING LICENSING OF NECESSARY CLAIMS:

If the Member owns, has a right to, or is aware of any Necessary Claims, please specify the patent number, patent application number and/or relevant claims.

• **Patent 1**

Patent name:

Method and apparatus for providing an adaptable security level in an electronic communication.

Patent application number(s):

Canada application filed 2,424,992 (7/7/03);

US provisional filed 60/484,656 (7/7/03), US application filed. App. No. 10/885,115 (7/7/04).

Relevant claims:

- 1) A method of communicating in a secure communication system, comprising the steps of:
 - a. Assembling as message at a sender;
 - b. Determining a security level;
 - c. Including an indication of the security level in a header of the message;
 - d. Sending the message to a recipient.
- 2) A method according to Claim 1 wherein the security level is chosen to be at least a minimum security level known to the sender and the recipient.



This declaration and all references to Certicom's Intellectual Property and licensing terms are Confidential information, per Clause 6 of the ZigBee Alliance Participation Agreement, and must be treated as such.

This information shall not be distributed outside the ZigBee Board of Directors, per Exhibit 2, Clause 3 (b) of the ZigBee Alliance Participation Agreement.

- 3) A method of communicating in a secure communication system, wherein each communication is divided into a plurality of frames, and each frame includes an indication of a security level, thereby allowing each frame to have a different security level to adapt to the nature of each frame.

Describe the nature, extent, and scope of the Necessary Claims (attach additional pages, if necessary):

The present claims are related to an encoding method of security-relevant information (in case: the security level) in a frame to be communicated by a sender in a secure communication system, such as to allow easy extraction of security-relevant information (in case: the security level) by its recipient(s), thus facilitating flexible cryptographic processing hereof.

• **Patent 2**

Patent name:

Cryptographic Method and Apparatus.

Patent application number(s):

Canada application filed 2,449,524 (11/14/03);

US Provisional filed 60/519,609 (11/14/03).

Relevant claims:

There are no claims included with this patent application at this time. As this patent application evolves, Certicom will notify the Zigbee Alliance of the addition of claims, as required.

Describe the nature, extent, and scope of the Necessary Claims (attach additional pages, if necessary):

There are no claims included with this patent application at this time. As this patent application evolves, Certicom will notify the Zigbee Alliance of the addition of claims, as required.

With respect to licensing such Necessary Claims, Member declares as follows (*check one box only*):

1. The Member is prepared to grant a Royalty Free License to the Alliance, Promoter Members and Participants.
2. **The Member will grant a fee-based license to the Alliance, Promoter Members and Participants on mutually acceptable terms and conditions to comply with the ZigBee Proposed Specification or Adopted Specification. (Member must provide the information requested in Attachment A to this Declaration)**
3. The Member disclosed the Necessary Claims of an Affiliate or Non-Member, but the Member is not authorized to grant licenses on behalf of such Affiliate or Non-Member according to the provisions of either 1 or 2 above.
4. The Member is not aware of any Necessary Claims.

E. SIGNATURE:

Print name of authorized person: Paul Carter

Title of authorized person: Director, IP Licensing Operations

Signature of authorized person: _____ Date: October 26, 2004



This declaration and all references to Certicom's Intellectual Property and licensing terms are *Confidential* information, per Clause 6 of the ZigBee Alliance Participation Agreement, and must be treated as such.

This information shall not be distributed outside the ZigBee Board of Directors, per Exhibit 2, Clause 3 (b) of the ZigBee Alliance Participation Agreement.

ATTACHMENT A

The information requested below is to be provided by any Member that checked **Box 2** of **Section D** (Position Regarding Licensing of Necessary Claims) of the Necessary Claims Declaration:

1. The Member shall disclose all portion(s) of the Proposed Specifications which involve any Necessary Claims (including without limitation, any Necessary Claims of an Affiliate or a Non-Member):

- **Patent 1 (as referenced above)**

This invention relates to an encoding method of security-related information in a frame to be communicated by a sender in a secure communication system, such as to allow easy extraction of security-relevant information by its recipient(s), thus facilitating flexible cryptographic processing hereof (e.g., taking into account purported protection level applied to the frame, key identifying information, algorithmic information, and other security-related information).

Portion(s) of the Proposed Specifications that involve Necessary Claims:

All outgoing and incoming frames that require security on the NWK Layer (Clause 5) and the APS Layer (Clause 6).

More particularly, this refers to clauses of the ZigBee Alliance Security Specification, v0.92 (03/322r12ZB), including the following:

Clause 5:

Frame Security (5.1), Secured NPDU Frame (5.2).

Clause 6:

Frame Security (6.1), Key Establishment (6.2), Transport-Key Services (6.3), Update-Device Services (6.4), Remove Device Services (6.5), Request Key Services (6.6), Switch Key Services (6.7), Secured APDU Frame (6.8), Command Frames (6.9).

Clause 7:

Common Frame Header Format (7.1). Security Parameters (7.2).

Clause 8:

Security Procedures (8.3).

- **Patent 2 (as referenced above)**

This invention relates to particular cryptographic mechanisms.

Portion(s) of the Proposed Specifications that involve Necessary Claims:



This declaration and all references to Certicom's Intellectual Property and licensing terms are *Confidential* information, per Clause 6 of the ZigBee Alliance Participation Agreement, and must be treated as such.

This information shall not be distributed outside the ZigBee Board of Directors, per Exhibit 2, Clause 3 (b) of the ZigBee Alliance Participation Agreement.

There are no claims included with this patent application at this time. As this patent application evolves, Certicom will notify the Zigbee Alliance of the addition of claims, as required.

2. The Member shall disclose any terms and conditions applicable to the license of any Necessary Claims (including without limitation, any Necessary Claims of an Affiliate or a Non-Member):

Certicom has two patent applications that are pertinent to the Zigbee Alliance Security Services Specification, Revision 12, 03/322r12ZB, v0.92. These patent applications, filed in Canada and the US, are listed in section D of this Declaration. Certicom will offer licenses to this technology at US\$0.005 (one half US cent) per Zigbee implementation that includes Zigbee Alliance Security Services Specification, Rev 12, 03/322r12ZB, v0.92. For example, if a manufacturer is developing a chip or device that implements the Zigbee Alliance Security Services Specification, Revision 12, 03/322r12ZB, v0.92, Certicom will receive a fee of US\$0.005 (one half US cent) for each chip or device. As an alternative, in order to simplify the overall pricing model, Certicom will consider pooling with other Zigbee Alliance members that are also declaring fee-based licensing of their Intellectual Property in Zigbee Alliance Specifications v0.92. In a pooling model, each holder of intellectual property in the pool will receive a to-be-negotiated portion of the overall fee that is commensurate with contribution.