Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14197
Date:	2010-01-28
Replaces:	
Document Type:	Disposition of Comments
Document Title:	Disposition of Comments on ISO/IEC CD 29180 (ITU-T X.usnsec-1)
Document Source:	SC 6/WG 7 Barcelona meeting
Project Number:	
Document Status:	As per the SC 6 Barcelona resolution 6.7.9, this document is circulated for information.
Action ID:	FYI
Due Date:	
No. of Pages:	14

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

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 535 Rev.1

English only

Original: English

Question(s): 6/17 Geneva, 16-25 September 2009

TEMPORARY DOCUMENT

Source: Editors

Title: Preliminary disposition of comments on X.usnsec-1 and ISO/IEC CD 29180

Contact: Heung Youl Youm
SoonChunhyang Univ.
Korea (Republic of)
Tel: +82 41 530 1328
Fax: +82 41 530 1494
Email: hyyoum@sch.ac.kr

Contact: Eunyoung Choi
KISA
Korea (Republic of)
Tel: +82-2-405-4706
Fax: +82-2-405-5219
Email: bluecey@kisa.or.kr

MB	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	Disposition
CN	Page 3		te	Node to node authentication is one basic security requirement in SN.	Add “node to node authentication” as one of Keywords.	Accepted
CN	Clause 6		te	Node to node communication is one basic communication patterns in SN.	Add an item “node to node communication” at the end of “The communication patterns within our SN fall into three categories:”.	Accepted
CN	Clause 6		te	It can not ignore the important communication pattern of Node communication with its neighbours in SN	Replace “The communication paradigm is either base station to sensor or sensor to base station.” as “The communication paradigm is base station to sensor, sensor to base station, sensor to its neighbours and node to node.”	Accepted
CN	Clause 7		ed	Spelling mistakes.	Replace “clause 7.1” as “clause 6.1”, replace “clause 7.2” as “clause 6.2” in clause 7.1.	Accepted
CN	Subclause 7.1.1		ed	Spelling mistakes.	Replace all “DOS” as “DoS” in subclause 7.1.1.	Accepted
CN	clause 8		te	Identification authentication is one important security requirement in SN.	Add the following after item “Data Authentication” : “Identification authentication: The authentication mechanisms are mainly used to validate the legitimacy of the node which to be communicating with, to ensure that the node is legitimate and credible.”	Accepted with modification At the end of data authentication, the proposed sentence was added since authentication is used for identification.
CN	Subclause 10.1	Paragraph 3	te	In the random key schemes presented thus far, no schemes can provide node to node authentication.	Add the following at the end of paragraph 2 at page 19: However, in the random key schemes presented thus far, while each node can verify that some of its neighbours have certain secret keys and are thus legitimate nodes, no node can authenticate the identity of a neighbour that it is communicating with.	Accepted
CN	Subclause 10.1		te	Key schemes should provide node to node authentication based on the pre-shared key.	Add a following item at the end of “The requirements of key management in a sensor network should be as follows:” Provide node to node identification authentication	Accepted
CN	Subclause 10.2		te	Does not present a whole description of broadcast authentication in SN.	Replace the Subclause 10.2 as following: 10.2 Authenticated broadcast It is important as broadcasts are used in many applications in sensor networks. For example, routing tree construction, network query, software updates, time synchronization, and network management all rely on broadcast. However, due to the nature of wireless communication in sensor networks, attackers can easily inject malicious data or alter the content of legitimate messages during multihop forwarding. Sensor networks applications need authentication mechanisms to	Partially accepted, Proposed comment are FFS and they will be considered at next meeting

					ensure the data from a valid source will not be altered during the transmission. Broadcast authentication is one of the most important security primitives in sensor networks. Basing on the employed cryptography, the broadcast authentication protocols which suit sensor networks are approximately divided into two groups. BiBa and HORS are those schemes which based on One Time Signature. For the main computation consist of one way hash functions, they are more efficient than public key signature schemes and can compare favourably with symmetric primitives. However, One Time Signature schemes have some drawbacks. Such as, limited number of signatures that one key pair can generate and the large size of the public key. Hence, it is still hard for them to satisfy the demand of sensor networks for the moment. Another type of broadcast authentication protocol bases on message authentication code (MAC). An efficient time based stream authentication scheme, called μTESLA which uses pure symmetric primitives to achieve asymmetric property by one way key chain. However, μTESLA has some constraints including time synchronization of the whole networks, inefficient unicast of the initial trust, and delayed authentication. Based on μTESLA, several extensions have been proposed, which enable the original μTESLA to cover a longtime period and support many receivers. But some constraints of μTESLA still existed, such as delayed authentication. The requirements of the authenticated broadcast in a sensor network should be as follows: **Resistance against node compromise:** Since it is unlikely that tamper-proof hardware will be deployed on sensor motes in the near future, secure sensor network protocols need to be resilient against compromised nodes **Low computation overhead:** Sensor nodes have limited computation resources, so an ideal protocol would have low computation overhead for both sender and receiver. **Low communication overhead:** Energy is an extremely scarce resource on sensor nodes. In particular, radio communication consumes the most amount of energy, and thus protocols with high communication overhead are avoided if possible. **Robustness to packet loss:** Reliable message delivery is the property of a network such that valid messages are not dropped. **Immediate authentication:** Depending on the application, authentication delay may influence the design of the sensor network protocol. For time-critical messages such as fire alarms, the receiver would most likely need to authenticate the	

					message immediately. However, authentication delay is typically acceptable for non-timecritical messages. The details on authenticated broadcast are described in ANNEX B.	
CN	Clause 10		te	Authentication mechanism is one basic security mechanism which should be considered in this CD document.	Add the following after Clause 10.7 10.8 Authentication mechanisms The authentication mechanisms are mainly used to validate the legitimacy of the equipment when it entering the network, to ensure that the equipments in the network are legitimate and credible. The details on authentication mechanisms are described in ANNEX C.	Accepted, with modification : annex to appendix
CN	Clause 11		te	Node to node authentication should be one of Mandatory Requirements for it is a basic security requirement in SN.	Add "The SN is required to authenticate the node identification of each other." at the end of clause 11.1.	Accepted
CN	Page 22		te	In order to carry out the work of the following, such as SN security specification, the framework of SN Security Specification is needed in this CD documents.	Add the following after Clause 11.3. **12 WSN Security Specifications** This section involves only the network layer and application layer security specifications. The MAC layer security referring to the MAC layer protocol will not be defined here. **12.1 Overview** The security services provided by the WSN include: key establishment, authentication, frame protection as well as node management. These services constitute an integral part of the security policy of WSN nodes. This chapter is a detailed description of the usage and the basic functions of these security services. **12.1.1 Network layer security** When the network layer frame is in need of protection, the frame protection mechanisms must be enabled in the node. The specific frame protection strategy is determined by the appointed security level. **12.1.2 Application layer security** When the application layer frame is in need of protection, the frame protection mechanisms must be enabled in the node. The specific frame protection strategy is determined by the appointed security level. The application layer also provides key management, node management, authentication and other security services. **12.2 Network layer security** The network layer processes the outgoing and incoming	Rejected, since current scope of this recommendation is focusing on requirements and key security functions, not specification of relevant layers, However, the scope of document will be reviewed again.

					frames which need to be protected. The safety operation of the network layer is controlled by the upper layer through establishing a suitable key and frame couter as well as setting up a security level. **12.2.1 Frame security** **12.2.1.1 Key** The keys used for protecting the network layer frame are provided by the upper layer. **12.2.1.2 Security processing of outgoing frames** **12.2.1.2.1 Encapsulation of non-broadcast frames** The non-broadcast frames include unicast and multicast frames, using the same frame protection mode as the MAC layer. **12.2.1.2.2 Encapsulation of the broadcast frames** The broadcast frame uses the message authentication code (MAC) for protection to ensure that the broadcast message is from the legitimate broadcaster and has not been tampered during the transmission, see ANNEX B. The MAC is calculated by the broadcast authentication key, and the key will be sent to the receiver after a pre-defined delay. **12.2.1.3 Security processing of incoming frames** **12.2.1.3.1 Decapsulation of non-broadcast frames** The decapsulation of the non-broadcast frame is resolved according to the security level of the incoming frames. **12.2.1.3.2 Decapsulation of the broadcast frame** The protected broadcast frames will be stored when received. The broadcast authentication key will be verified by the existing key which came from the broadcast authentication key chain after received, see ANNEX B. Then the broadcast frame will be authenticated basing on the broadcast authentication key. **12.2.2 The format of the safety frame** According to the format of the network layer frame, the security control domain field is added to constitute the safety network layer frame. **12.2.3 Security-related NIB (Network layer Information B** **ase) attributes** It refers to the security-related NIB attributes. **12.3 Application layer security** The network layer is responsible for processing the outgoing and incoming frames which need to be protected, as well as	

					key management and node management. **12.3.1 Key management services** In this section, the key management refers to the management of the pre-distributed key. **12.3.1.1 Key establishment** The key establishment procedure can be found in ANNEX A. **12.3.1.2 Key maintenance** **12.3.2 Entity authentication services** The specific authentication mechanism is realized by the authentication suites, see ANNEX C. In ID-based authentication procedure, the nodes use ECDH exchange to negociate a base key BK; in preshared key authentication procedure, the nodes using their shared key as a seed to export the base key BK. Then, in the unicast key negociation procedure, the nodes exchange respectively a random number between them and export the unicast session key based on BK. Finally, in the multicast key announcement procedure, the nodes expand respectively the NMK(notification master key) to generate the multicast session key(the multicast key is only used by the sink node). **12.3.3 Frame security** **12.3.3.1 Key** The safety of outgoing and incoming frame is ensured by the key produced by the authentication services. **12.3.3.2 Security processing of outgoing frames** It uses the same frame protection mode as the MAC layer. **12.3.3.3 Security processing of incoming frames** It resolves according to the security level of the received frame. **12.3.4 Command frames** It defines the format of the command frames for various security services. **12.3.5 Node management services** **13.3.5.1 Node update** It provides a safe way to inform a node the status updating information of other nodes. **12.3.5.2 Node delete** It provides a safe way to inform a node to delete information of other nodes.	

					12.3.6 AIB (Application Information Base) security-related attribute It defines the AIB security-related attributes. **12.3.7 Public safety element** The format of the head of the security frame includes security control field, frame counter,source address, key serial number,etc. **12.3.8 Functional description** This sub-clause provides detailed descriptions of how the security services shall be used in a WSN.	
CN	ANNEX A		te	A key scheme providing node to node authentication is needed in Key management methods in Sensor Networks.	Add the following in ANNEX A. **A.3.1.6 PROBABILISTIC PAIR-WISE KEY PRE-DISTR IBUTION** The probabilistic pair-wise keys scheme is a modification of the pair-wise key scheme based on the observation that not all n-1 keys need to be stored in the node's key ring to have a connected random graph with high probability. Erd¨os and R´enyi's formula allows us to calculate the smallest probability p of any two nodes being connected such that the entire graph is connected with high probability c. To achieve this probability p in a network with n nodes, each node need only store a random set of np pair-wise key instead of exhaustively storing all n-1. The use of pair-wise keys instead of purely random keys chosen from a given pool can give us node-to-node authentication properties if each node which holds some key k, also stores the identity (ID) of the other node which also holds k. Hence, if k is used to create a secure link with another node, both nodes are certain of the identity of each other since no other nodes can hold k.	Accepted
CN	Page 25		te	Like ANNEX A, there needs to give a detailed description of broadcast authentication in SN.	Add the following after ANNEX A. **ANNEX B** **Authenticated broadcast in Sensor Networks** **B.1 Construction of µTPC** The essential problem to scaling up µTESLA is how to distribute and authenticate the initial µTESLA parameters (µTP), mainly including the key chain commitments, starting time, duration of each time interval, etc. The multi-level µTESLA uses high-level µTESLA instances to authenticate	Accepted with change from annex to appendix since the specific protocol should be appendix.

					the parameters of low-level ones. It inherits the authentication delay introduced by µTESLA during the distribution of those parameters. The consequence of such authentication delay is that an attacker can launch DoS attacks to disrupt the distribution of initial µTESLA parameters. Moreover, multi-level µTESLA cannot handle a large number of senders. Tree-based µTESLA protocol uses Merkle Tree mechanism to distribute µTP. Using the certificate from Merkle tree, receiver nodes can authenticate µTP immediately, so it can resist DoS attacks. But the cost of Tree-based µTESLA is too large. The µTPCT-based broadcast authentication protocol constructs µTPC (µTP one way Chain) to distribute and authenticate µTP. It can resist DoS attacks and only need small cost. In sensor networks with multiple BNodes, in view of the task to be performed, BNode (Broadcast Node) may have different characteristics. The life cycle, broadcasting frequency and real-time requirement of BNode are as Feature Parameters, for short as FP. BS (Base Station) will construct µTP based on the FP of BNode. For example, for the BNode with short life cycle, high broadcasting frequency and strong real-time requirement, BS will construct a special µTP which contains short key disclosure lag and less µTESLA instances with short time interval. FP can be expanded as required. µTPC is composed of µTP and One Way Chain. After FP is determined, BS will firstly divide the lifetime of BNode into N time intervals with length of T_N, such that the duration of T_N (e.g., 30 minutes) is suitable for running a µTESLA instance on a BNode and sensor nodes efficiently. According to broadcasting frequency and real-time requirement of BNode, BS will divide T_N into n time interval with length of T_n. Bases on N and n, BS uses pseudo-random function F to generate N µTESLA key chains which linked together. At first, BS generates the last key $K_{N,n}$ of the N-th µTESLA key chain at randomly. Then using hash function H (e.g., SHA-1), BS generates rest keys of the N-th µTESLA key chain according to $K_{N,i}=H(K_{N,i+1})$. For the (i-1)-th µTESLA key chain, BS generates the last key by performing a pseudo random function on the first key (the key next to the commitment) of the i-th µTESLA key chain, then generates rest keys of (i-1)-th µTESLA key chain by performing H on it's last key. By this way, BS generate all µTESLA key chains till to the last one. Figure B-1 shows the construction of µTESLA key chains. After all µTESLA key chains was generated, for the BNode j, BS will assign different keys to different time intervals T_n. Accordingly, there will come into being N µTESLA instances. Where the initial parameter of the ith µTESLA instance is $\mu TP_i=\{T_s \quad K_{i,0} \quad T_i \quad T_{int} \quad d\}$, where T_s denotes current time, $K_{i,0}$ denotes the commitment, T_i denotes starting time, T_{int} denotes synchronization interval, d denotes disclosure lag of the key. After all µTP were determined, BS generates a value U_N	

randomly, then computes each U value by U_{i-1}= H(U_i μTP_{i-1}) till to U_0. Where, " " denotes message concatenation. Finally, BS constructs a µTPC which including N µTPs. Figure B-2 shows an example of construction of µTPC.

B.2 Construction of µTPCT

Suppose m BNodes exist in sensor networks. For convenience, we assume $m = 2^k$, where k is an integer. Before deployment, BS pre-computes m µTPC, each of which is assigned a unique and integer-valued ID between 1 and m. For the sake of presentation, we denote the j-th U value of i-th µTPC as $U_{i,j}$, the j-th µTP as $\mu TP_{i,j,}$ the i-th initial parameter (including $U_{i,0}$, ID_i) of µTPC as S_i. BS then computes K_i=H(S_i) for all $i \in \{1,...,m\}$.Then, it constructs a Merkle tree using $\{K_1,...,K_m\}$ as leaf nodes. Each non-leaf node is computed by applying H to the concatenation of its children nodes. We call such a Merkle tree as µTPCT (µTPC merkle hash Tree). Figure B-3 shows a µTPCT with eight µTPC, where K_{12}=H(K_1 K_2), K_{14}=H(K_{12} K_{34}), K_{18}=H(K_{14} K_{58}), etc.

BS also constructs a parameter certificate for each µTPC instance. The certificate for i-th µTPC instance consists of S_i and the values corresponding to the siblings of the nodes on the path from i-th leaf node to the root of µTPCT. For example, the parameter certificate for the 4th µTPC instance in Figure B-3 is $PCert_4$={S_4,K_3,K_{12},K_{58}}. For each BNode which will use a given µTPC instance, BS distributes the µTPC and the corresponding parameter certificate to it. BS also pre-distributes the root of the µTPCT to all potentially receivers of broadcast messages.

Before construction of µTPCT, if there are same parts in all µTP of some µTPC, take the same parts of µTP together with initial parameter of µTPC as leaf nodes to construct µTPCT. For example, if the disclosure lag d and synchronization intervals T_{int} in all µTP of μTPC_i are same, take T_{int}, d together with initial parameter of μTPC_i as leaf nodes to construct µTPCT. Accordingly, the same parts of µTP will be distributed together with the certificate of µTPC with only one time. In the process of µTP distribution, BNode needs to distribute the discrepant part only. By this way, substantive communication cost will be saved.

B.3 Authenticated broadcast

The performing of Authenticated broadcast protocol can be divided into five phases as following.

1 Protocol initialization

Before the deployment of sensor networks, BS builds µTinst (denotes µTESLA instance), µTPC and µTPCT according to the quantity and FP of all BNodes. Then it distributes root R of

					µTPCT to RNode (Receiving Node). **2 Request µTPC** Before joining sensor networks, BNode sends request BREQ which includes BNode's FP to BS. Then, BS searches for the compatible µTPC (e.g. μTPC_4 shown in Figure 3) according to the FP of BNode. Together with certificate $PCert_4$ and K_{gen} (denotes the generate key of µTESLA key chain) of all µTinst, BS sends µTPC back to BNode. **3 Authenticate BNode** Before broadcasting, BNode publishes its certificate $PCert_4$ to all RNodes to prove its legitimacy. RNode using R and equation H(H(H(H(S_4) K_3) K_{12}) K_{58})=K_{18} to verify the validity of $PCert_4$. If succeeds, RNode saves µTPC's initial parameter $U_{4,0}$, ID_4 consist in $PCert_4$ and the same parts of µTP in µTPC. **4 Distribute µTP** After successfully authenticated, BNode creates first µTESLA key chain according to K_{gen} of the first µTinst using hash function H. Then, BNode broadcasts $U_{4,1}$ and $\mu TP_{4,0}$ to RNodes. According to $U_{4,0}$=H($U_{4,1}$ $\mu TP_{4,0}$), RNode verifies the legitimacy of $\mu TP_{4,0}$. If succeeds, RNode saves $U_{4,1}$ and $\mu TP_{4,0}$, otherwise, discards it. Then, BNode broadcasts $U_{4,2}$ successively. At the same time, BNode uses the 2nd K_{gen} to generate second µTESLA key chain. After receiving $U_{4,2}$, RNode saves it and deletes $U_{4,0}$. To assure the reliability of the distribution, BNode will broadcast U repeatedly. **5 Authenticate broadcast message** Once RNode gained $\mu TP_{4,0}$, bases on $\mu Tinst_{4,0}$, RNode can authenticate all broadcast message from BNode. Therefore, a broadcast authentication channel comes into being between RNode and BNode. When there left 2*T_{int} time to the ending of life cycle of $\mu Tinst_{4,0}$ in the processing of broadcast authentication, the protocol will go to performing phase 4 subsequently. That is, BNode broadcasts $\mu TP_{4,1}$. RNode verifies $\mu TP_{4,1}$ using $U_{4,1}$=H($U_{4,2}$ $\mu TP_{4,1}$). If succeeds, RNode saves $\mu TP_{4,1}$, otherwise, discards it. By this way, the protocol makes sure that RNode can continue to authenticate broadcast message of BNode in the life cycle of $\mu Tinst_{4,1}$. The later procedure of the protocol will repeat phase 5 till life of BNode finished.	
CN	Page 25		te	Like ANNEX A, there needs to give a detailed description of authentication mechanisms in SN.	Add the following after ANNEX B. **ANNEX C** **Authentication mechanisms in Sensor Networks**	Accepted with modification from annex to appendix

C.1 Preshared Key based authentication

See Figure C-1.

In the following text, the PSK denotes the preshared key between A and B, the "$ADDID_x$" denotes the concatenation of A's address and B's address. The mechanism is performed as follows:

Step 1: B sends an "AUTH REQUEST" message to A to start the authentication procedure;

Step 2: After receiving the message, A generates a nonce N_A and sends it to B;

Step 3: B generates a nonce N_B and calculates the session key SK=KD-HMAC-SHA256(PSK,$ADDID_1||N_B||N_A||$"pairwise key expansion for unicast and additional keys and nonce") and a message authentication code MAC_1=KD-HMAC-SHA256(SK, $N_B||N_A$), then sends MAC_1,N_B and N_A to A;

Step4: A checks N_A firstly, then calculates SK=KD-HMAC-SHA256(PSK, $ADDID_2||N_B||N_A||$"pairwise key expansion for unicast and additional keys and nonce"), and MAC_2=KD-HMAC-SHA256(SK, $N_B||N_A$). If MAC_1= MAC_2, A sends MAC_3=KD-HMAC-SHA256(SK,N_B) and N_B to B;

C.2 ID-based authentication

See Figure C-2.

In the following text, $PubKey_X$ denotes the public key of X. SIG_X denotes the signature of X. Res ($PubKey_X$) denotes the result of verification of $PubKey_X$. The mechanism is performed as follows:

Step 1: A generates a random number N_A and sends $N_A||PubKey_A$ to B;

Step 2: B generates a temporal secret key x and a temporal public key x·P for ECDH, then sends $N_A||N_B||x·P||PubKey_B||SIG_B(N_A||N_B||x·P||PubKey_A)$ to A;

Step 3: After receiving the message from B, A generates another random number N_A' and sends $N_B||N_A'||PubKey_A||PubKey_B$ to T;

					Step 4: On receipt of the message from A, T inspects the validity of $PubKey_A$ and $PubKey_B$, and sends N_A'||Res($PubKey_A$)||Res($PubKey_B$)||SIG_T(N_B||Res($PubKey_A$))||SIG_T(N_A'||Res($PubKey_B$)) to A; **Step 5**: After receiving the message from T, A verifies N_A' firstly, then verifies SIG_T(N_A'||Res($PubKey_B$)) by checking if N_A' agrees with the one sent to T. Then A generates a temporal secret key y and a temporal public key y·P for ECDH, calculates BK_{AB}=KD-HMAC-SHA256((x·y·P)abscissa, NA||NB|| "base key expansion for key and additional nonce"), and sends N_B||y·P||Res($PubKey_A$)||SIG_A(N_B||y·P||$PubKey_B$)|| SIG_T(N_B||Res($PubKey_A$)) to B; **Step 6**: B verifies N_B firstly, then verifies SIG_T(N_B||Res($PubKey_A$)) and SIG_A(N_B||y·P||$PubKey_B$) by checking N_A and N_B respectively. Then B calculates the Base Key BK_{AB}=KD-HMAC-SHA256((x·y·P)abscissa, NA||NB|| "base key expansion for key and additional nonce"). Basing on the BK_{AB}, B calculates MAC= KD-HMAC-SHA256(BK_{AB}, N_A) and then sends it with N_A to A. A verifies the MAC from B basing on the BK_{AB}.	
DE 1	4		ed	List of Abbreviation is incomplete!	e.g. missing abbreviations: NGN, NMS, distinction between Sensor Node and SensorNetwork, …	Accepted
DE 2	9.1		te	the intention of the Mapping Tables of section 9.1 is unclear By 5 tables 8 security dimensions (identical with security requirements?) are mapped onto 5 threat groups. The grouping is a combination of message exchange pattern in SN and a kind of Target of Evaluation (e.g. Information Security, Sensor Node, Base Station Broadcasting, Insider Routing Information, Outsider Routing Information). Some Security Threats are marked to "be opposed" to security requirements (dimensions?). It should be more precisely outlined why some threats are opposed to requirements and some others are not. e.g. one can learn from these tables that e.g the security requirement "access control" is opposed to destruction, corruption, theft and loss and disclosure of information (table 1), is not applicable to node specific threats (table 2), is opposed to threats against broadcasting messages (table 3), is opposed to threats of insider attacks, i.e. sybil attack, HELLO flood, Wormholde, Sinkhole, Selective Forwarding (table 4) and is opposed to selective forwarding of an outsider attack		Proposed comment are FFS and they will be considered at next meeting

				(table 5).		
DE 3	10.2		te	missing reference to the RFC 4082 TESLA Protocol Specification	In section 10.2 the TESLA Algorithm is introduced. Instead of referencing to the recent IETF standard RFC 4082, it is referred to basic publications of the year 2000. The TESLA protocol sketch in section 10.2 deviates from the specification of RFC 4082 in certain definitions and explanations. In the standard there should be one (standard) reference that explains the algorithm.	Accepted
DE 4	10.5 10.6		te	missing relationship to notions of CC/FIPS standards:	The General Model of the CC part 1/2 contains a specification of “Security Requirements” which need to be related to the Security Requirements/Dimensions of the USN Security Document (6N13711). Similar to the definition of USN Security Requirements the CC Model defines Security Targets, Target of Evaluation, Countermeasures and Threats. These notions are related to identified assets, (whereas definition and usage of Asset is missing in the 6N13711 document). a. To section 10.5 “Tamper-resistant Module (TRM)” and section 10.6 “USN Middleware Security” the notion of the “Cryptographic Module (CM)” of the CC/FIPS standards is very relevant. b. The CM is a tamper-resistant module which ensures sensitive date whithout storage damage and thus shall be considered as TRM and as a middleware security module.	Proposed comment are FFS and they will be considered at next meeting

_____