**IEEE P802.21
Media Independent Handover Services**

|  |
| --- |
| **The data format of SIGNATURE**  |
| **Date:** 2013-09-17 |
| **Author(s):** |
| **Name** | **Affiliation** | **Address** | **Phone** | **Email** |
| Yoshikazu Hanatani | Toshiba |  |  | yoshikazu.hanatani@ toshiba.co.jp |

Abstract

This document contains proposed remedy for “the 802.21d ballot 7 comment #173 about the data format of SIGNATUE.

To detect a verification key, SIGNATURE TLV includes “CERT\_SERIAL\_NUMBER” and “SIGNATURE”**.** If CERT\_SETIAL\_NUMBER of a X.509 certificate is obtained, we can detect the verification key and the verification algorithm from the X.509 certificate.

Insert a following text about generating SIGNATURE TLV to an appropriate part. (It is the part on an operation of PoS’s MIHF in section 9.4.2?).

“The MIHF of PoS generates a Signature TLV consisting of a SIGNATURE\_DATA and a CERT\_SERIAL\_NUMBER. The SIGNATURE\_DATA is created by signing to an MIH group manipulate command and an MIH group addressed command using a signing key corresponding with a verification key specified by CERT\_SERIAL\_NUMBER.”

Insert a following text about verifying SIGNATURE TLV to an appropriate part. (It is the pert on an operation of MN’s MIHF in section 9.4.2?)

“The MIHF of MN retrieves CERT\_SERIAL\_NUMBER and SIGNATURE\_DATA from the SIGNATURE\_TLV. Then, the MIHF verifies the SIGNATURE\_DATA using a verification key specified by the CERT\_SERIAL\_NUMBER.”

In order to add CERT\_SERIAL\_NUMBER to SIGNATURE TLV, the data type of SIGNATURE is changed.

* + 1. **Data type for security**

***Change Table F.24 as follows:***

**Table F.24—Data type for security**

|  |  |  |
| --- | --- | --- |
| **Data type name**  | **Derived from** | **Definition** |
| SIGNATURE | SEQUENCE(CERT\_SERIAL\_NUMBER,SIGNATURE\_DATA) | The OCTET\_STRING is a digital signature data which is verified by a verification key indicated by the CERT\_SERIAL\_NUMBER. |