# IEEE P802.21 Media Independent Handover Services

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bootstrapping Commands for IEEE 802.21a Credential | | | | |
| Date: 2013-05-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Yoshikazu Hanatani | Toshiba Corporation | 1 Komukai-Toshiba-cho, Saiwai-ku, Kawasaki, 212-8582 Japan |  | [yoshikazu.hanatani@toshiba.co.jp](mailto:yoshikazu.hanatani@toshiba.co.jp) |
| Toru Kambayashi | Toshiba Corporation | 1 Komukai-Toshiba-cho, Saiwai-ku, Kawasaki, 212-8582 Japan |  | [tooru.kamibayashi@toshiba.co.jp](mailto:tooru.kamibayashi@toshiba.co.jp) |

Abstract

This proposal is a contribution for the 802.21d in response to 802.21-12-0091-06-MuGM-requirements-document. This proposal presents primitives and messages to deliver a credential of IEEE 802.21a to an MN.

Section numbering in this document corresponds to the one in IEEE 802.21-2008.

# Overview

# Normative references

# Definitions

# Abbreviations and acronyms

# General architecture

## Introduction

## General design principles

## MIHF service overview

## Media independent handover reference framework

## MIHF reference models for link-layer technologies

## Service access points (SAPs)

## MIH protocol

# MIHF services

## General

## Service management

## Media independent event service

## Media independent command service

### Introduction

### Command service flow model

### Command lists

## Media independent information service

# Service access points (SAPs) and primitives

## Introduction

## SAPs

## MIH\_LINK\_SAP primitives

## MIH\_SAP primitives

### MIH\_Pull\_Certedential

* + - 1. MIH\_Pull\_Credential.request
         1. Function

This primitive is generated by an MN used to request to send a certificate from the PoS to a destination PoS or MN.

* + - * 1. Semantics of service primitive

MIH\_Pull\_Credential.request (

DestinationIdentifier,

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MIHF\_ID | Specifies the sender of the credential. |

* + - * 1. When generated

An MN generates this primitive for requesting a credential or for credential updates.

* + - * 1. Effect on receipt

Upon receipt of this primitive, the MIHF on the MN sends the corresponding MIH\_Pull\_Credential request message to the destination MN or PoS.

* + - 1. MIH\_Pull\_Certificate.indication
         1. Function

This primitive is generated by an MIHF that receives an MIH\_Pull\_Credential request message in order to inform a credential requester to an MIH User.

* + - * 1. Semantics of service primitive

MIH\_Pull\_Credential.indication (

SourceIdentifier,

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MIHF\_ID | Identifies the requester of the certificate. |

* + - * 1. When generated

This primitive is generated by an MIHF when an MIH\_Pull\_Credential request message is received.

* + - * 1. Effect on receipt

Upon receipt of this primitive, the MIH user generates MIH\_Pull\_Credential.response to deliver a credential to the credential requester.

* + - 1. MIH\_Pull\_Credential.response
         1. Function

This primitive is generated by an MIH User in order to deliver a credential for IEEE 802.21a to MN or other PoS.

* + - * 1. Semantics of service primitive

MIH\_Pull\_Credential.response (

DestinationIdentifier,

Credential

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MIHF\_ID | Specifies the requestor of the credential. |
| Credential | CERTIFICATE | X.509 certificate |

* + - * 1. When generated

An MIH User generates this primitive using a leaf key corresponding with the certificate requester.

* + - * 1. Effect on receipt

Upon receipt of this primitive, the MIHF on the PoS generates MIH\_Pull\_Credential response message to the destination MN or PoS.

* + - 1. MIH\_Pull\_Credential.confirm
         1. Function

This primitive is generated by a MIHF that receives an MIH\_Credential response to indicate the credential.

* + - * 1. Semantics of service primitive

MIH\_Pull\_Credential.confirm (

SourceIdentifier,

Credential

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MIHF\_ID | Identifies the remote MIHF that invoked MIH\_Revoke\_Credential response. |
| Credential | CERTIFICATE | X.509 certificate |

* + - * 1. When generated

The MIHF that receives an MIH\_Pull\_Credential response message generates this primitive to indicate the credential.

* + - * 1. Effect on receipt

After verification, validated credential keys within their expiration period can be utilized for IEEE 802.21a.

* + 1. MIH\_Push\_Credential
       1. MIH\_Push\_Credential.request
          1. Function

This primitive is generated by a PoS used to send a credential from the PoS to a destination PoS or MN.

* + - * 1. Semantics of service primitive

MIH\_Push\_Credential.request (

DestinationIdentifier,

Credential

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MIHF\_ID | Specifies the recipient of the credential. |
| Credential | CERTIFICATE | X.509 certificate |

* + - * 1. When generated

A PoS generates this primitive for initial provisioning of certificates or for certificate updates.

* + - * 1. Effect on receipt

Upon receipt of this primitive, the MIHF on the PoS sends the corresponding MIH\_Push\_Credential request message to the destination MN or PoS.

* + - 1. MIH\_Push\_Credential.indication
         1. Function

This primitive is generated by a MIHF that receives an MIH\_Push\_Credential request message to manipulate group membership of one or more MN(s) or other PoS(es).

* + - * 1. Semantics of service primitive

MIH\_Push\_Credential.indication (

SourceIdentifier,

Credential

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MIHF\_ID | Identifies the sender of the credential. |
| Credential | CERTIFICATE | X.509 certificate |

* + - * 1. When generated

This primitive is generated by an MIHF when an MIH\_Push\_Credential request message is received.

* + - * 1. Effect on receipt

Credential signature is verified and result of verification is provided back to push requester. After verification, validated credential keys within their expiration period can be utilized for IEEE 802.21a.

* + - 1. MIH\_Push\_Credential.response
         1. Function

This primitive is generated by an MIH User to acknowledge receipt of a credential from a PoS.

* + - * 1. Semantics of service primitive

MIH\_Push\_Credential.response (

DestinationIdentifier,

CredentialSerialNumber,

CredentialStatus

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| DestinationIdentifier | MIHF\_ID | Specifies the sender of the credential. |
| CredentialSerialNumber | CERTIFICATE\_SERIAL\_NUMBER | X.509 certificate subfield – serial number |
| CredentialStatus | CERT\_STATUS | Indicates whether a certificate has been verified and is now in use by the recipient. |

* + - * 1. When generated

An MIH User generates this primitive after receipt and processing of certificate.

* + - * 1. Effect on receipt

If certificate signature is valid, then MIH\_Push\_Credential response message is sent back to the push requester. Result of request is provided in the REVOCATION\_STATUS.

* + - 1. MIH\_Push\_Certificate.confirm
         1. Function

This primitive is generated by a MIHF that receives an MIH\_Push\_Credential response to indicate the status of the certificate inspection.

* + - * 1. Semantics of service primitive

MIH\_Push\_Certificate.confirm (

SourceIdentifier,

CredentialNumber,

CredentialStatus

)

Parameters:

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Description |
| SourceIdentifier | MIHF\_ID | Identifies the remote MIHF that invoked MIH\_Push\_Credential response. |
| CredentialNumber | CERT\_SERIAL\_NUMBER | X.509 certificate subfield – serial number |
| CredentialStatus | CERT\_STATUS | Indicates whether a certificate has been verified and is now in use by the recipient. |

* + - * 1. When generated

The MIHF that receives an MIH\_Push\_Credential response message generates this primitive to indicate the status of the certificate inspection.

* + - * 1. Effect on receipt

If Credential Status indicates success indicates that the PoS can manage device as being capable of authenticated by IEEE 802.21a mechanism.

## MIH\_NET\_SAP primitives

# Media independent handover protocol

## Introduction

## MIH protocol description

### MIH protocol transaction

### MIH protocol acknowledgement service

### MIH protocol transaction state diagram

### Other considerations

## MIH protocol identifiers

### MIHF ID

### Transaction ID

## MIH protocol frame format

### General frame format

#### 8.4.1a.1 MIH PDU protected by (D)TLS

#### 8.4.1a.2 MIH PDU protected through EAP-generated MIH SA

#### 8.4.1a.3 MIH PDU protected through GKB-generated MIH SA

#### 8.4.1a.4 Protected MIH PDU upon transport address change

### Fragmentation and reassembly

## Message parameter TLV encoding

## MIH protocol messages

### MIH messages for service management

### MIH messages for event service

### MIH messages for command service

* + - 1. MIH\_Pull\_Credential request

The corresponding MIH primitive of this message is defined in XXXX.

This message is used by the MIHF to request a credential to the PoS identified by the Destination Identifier.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=1, AID=XX ) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |

* + - 1. MIH\_Pull\_Credential response

The corresponding MIH primitive of this message is defined in XXXX.

This message is used by the MIHF to deliver a credential from a PoS.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=2, AID=XX ) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| EncryptedCredential (EncryptedCredential TLV) |

* + - 1. MIH\_Push\_Credential request

The corresponding MIH primitive of this message is defined in XXXX.

This message is used by the MIHF to deliver a credential encrypted by the leaf key that the MIH node identified by the Destination Identifier holds to the MIH node.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=1, AID=XX ) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| EncryptedCredential  (Encrypted Credential TLV) |

* + - 1. MIH\_Push\_Ceredential response

The corresponding MIH primitive of this message is defined in XXXX.

This message is used by the MIHF to acknowledge receipt of a certificate from a PoS.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=2, AID=XX ) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| CertificateSerialNumber  (Certificate Serial Number TLV) |
| CertificateStatus  (Certificate Status TLV) |

# MIH protocol protection\*

## Protection established through MIH (D)TLS

## Key establishment through an MIH service access authentication

## MIH message protection mechanisms for EAP-generated SAs

## Multicast MIH message protection mechanisms

### MIH message protection mechanisms for GKB-generated SAs

### Secure group manipulation with group key distribution

### GKB operation by the complete subtree method

### Encapsulation

### Decapsulation

### Multicast message encryption based on group key

### Signature and Certificate Management

#### Multicast Message Signatures

#### Signature Verification

#### Certificate Management

### Multicast Ciphersuites

## Common procedures *(originally section 9.4)*

### Sending *(originally section 9.4.1)*

### Receiving *(originally section 9.4.2)*

# Annex F Data type definition

# The type of credential is CERTIFICATE (= X.509 certificate) only. Should we support other types of credential?

# Annex L MIH protocol message code assignment

***Modify Table L.1 as follows:***

1. —AID assignment

|  |  |
| --- | --- |
| MIH messages | AID |
| MIH messages for Command Service | |
| MIH\_Pull\_Credential | TBD |
| MIH\_Push\_Credential | TBD |

***Modify Table L.2 as follows:***

1. —Type values for TLV encoding

|  |  |  |
| --- | --- | --- |
| TLV type name | TLV type value | Data Type |
| EncryptedCredential | TBD | ENCR\_BLOCKDATA |

# Annex P MKB Toy Example