|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | SCV-TD121 |
|  |
| **Original: English** |
|  |  | Virtual, 3 June 2020 |
| **TD****(Ref.: SG9-LS105)** |
| **Source:** | ITU-T SG9 |
| **Title:** | LS/r on approval of new terms and definitions (SCV-LS26) [to SCV/CCV, all ITU-T Study Groups] |
| **Purpose:** |  |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For comment to:** | - |
| **For information to:** | SCV/CCV, All ITU-T study groups |
| **Approval:**  | **ITU-T SG9 meeting (E-meeting, 23 April 2020)** |
| **Deadline:** | N/A |
| **Contact:** | Zhongzhao LiABP, NRTAChina  | Tel: +86 10 86093737Fax: +86 10 86093658E-mail: lizhongzhao@abp2003.cn |
| **Contact:** | Satoshi MiyajiKDDI CorporationJapan | Tel: +81 3 6328 1905 Fax: +81 3 6757 1271E-mail: sa-miyaji@kddi.com  |

|  |  |
| --- | --- |
| **Keywords:** | SCV; terms and definitions |
| **Abstract:** | This liaison statement contains the reply of ITU-SG9 on new terms and definitions. |

ITU-T SG9 thanks SCV/CCV and ITU-T SGs for the alignment terms and definitions work.

At the ITU-T SG9 meeting (E-meeting, 16-23 April 2020), we review the liaison statement sent from SCV(Ref: [SCV-LS26](http://handle.itu.int/11.1002/ls/sp16-scv-oLS-00026.docx)) and fully support and follow the request to send to SCV and to SGs new terms and definitions before its approval.

At this meeting, we are developing new definitions for the following terms:

1. **RF log(J.acs-stb)**: Data log which consists of record of receive conditions at radio frequency equivalent to TV channel selected by STB user.
2. **standby mode(J.acs-stb)**: The mode that STB is not active in providing service to its user such as TV program and so on. Standby mode and active mode are generally switched each other by pressing the power button of STB itself or STB controller.
3. **Section(J.1211)**: Section is a syntactic structure used for mapping all service information defined in Recommendation ITU-T J.ipvb-spec into ITU-T H.222.0 | ISO/IEC 13818-1 TS packets
4. **Service(J.1211)**: Service is a series of programs which is broadcasted in stages according to a time schedule under the control of the broadcaster.
5. **Service Information (J.1211)**: Service information in this Recommendation describes the data information such as delivery systems, contents and plans/schedules of broadcast data streams, etc., including PSI information of MPEG-2 and independently defined extensions.
6. **IP broadcast** (J.1211): IP broadcast in this Recommendation refers to the implementation of the broadcast transmission of the baseband stream of IP on the CATV distribution network.
7. **Broadcast channel** (J.1211): The broadcast channels in this Recommendation refer to the logical channels labelled with D-class IP addresses and UDP destination port numbers. Usually one channel corresponds to a digital TV transmission stream or service stream.
8. **Main channel (J.1211)**: The main channel in this Recommendation refers to the broadcast channels delivering the digital TV service index data of IPVB.
9. **DRM App (J.stvos-spec)**: An application running in TVOS that executes none-secure sensitive DRM functionalities such as communication with DRM head end and retrieving content authorization. TVOS can manage multiple DRM applications to support different DRM services from different service providers.
10. **DRM TApp (J.stvos-spec)**: A trusted application running in TVOS trusted execution environment that executes secure DRM functionalities such as content decryption, secure video path and trust chain verification.
11. **DCAS App (J.stvos-spec)**: An application running in TVOS that executes none-secure sensitive DCAS functionalities such as setting filter to get ECM/EMM packet from transport stream, and sending ECM/EMM to DCAS TApp. TVOS can manage multiple DCAS applications to support different DCAS services from different service providers.
12. **DCAS TApp (J.stvos-spec)**: A trusted application running in TVOS trusted execution environment that executes secure DCAS functionalities such as ECM/EMM packet decryption and signature verification.
13. **Advanced Security System (AS System)（J.1012）:** Function of an ECI compliant CPE, which provides enhanced security functions (hardware and software) for an ECI Client.
14. **AS slot（J.1012）:** Resources of the advanced security block provided exclusively to an ECI client by the ECI Host.
15. **AS slot session（J.1012）:** Resources and computing in an AS slot related to the de-cryption or re‑encryption of a content element.
16. **Brother（J.1012）:** Other Child of the same Father.

 NOTE – Father, Children, Brother refer to entities that manage Certificates.

1. **Certificate（J.1012）:** Data structure as defined in clause 5 of this Recommendation with a complementary secure digital signature that identifies an Entity.

 NOTE – The holder of the secret key of the signature attests to the correctness of the data - authenticates it - by signing it with its secret key. Its public key can be used to verify the data.

1. **Certificate Chain（J.1012）:** List of Certificates that authenticate each other up to and including a root revocation list.
2. **Certificate Processing Subsystem (CPS) （J.1012）:** Subsystem of the ECI Host that provides Certificate verification processing and providing additional robustness against tampering.
3. **Child, Children（J.1012）:** Entity (entities) referred to by a Certificate signed by a (common) Father.

 NOTE – Father, Children, Brother are referring to entities that manage Certificates: initialization data and software that is used to start the SoC of a CPE.

1. **Content Protection system（J.1012）:** System in an ECI Ecosystem that employs cryptographic techniques to manage access to content and services.

 NOTE – The term may be interchanged frequently with the alternate service protection system. Typical systems of this sort are either conditional access systems (CAS), or digital rights management systems (DRM).

1. **Customer Premises Equipment (CPE) （J.1012）:** Media receiver which has implemented ECI, allowing the User to access digital media services.
2. **CPE manufacturer（J.1012）:** A company that manufactures ECI compliant CPEs.
3. **ECI (Embedded CI) （J.1012）:** Architecture and the system specified in the ETSI ISG "Embedded CI", which allows the development and implementation of software-based swappable ECI Clients in customer premises equipment (CPE) and thus provides interoperability of CPE devices with respect to ECI.
4. **ECI application（J.1012）:** HTML based application hosted on an ECI Client, and running in a dedicated browser session for the purpose of interacting with the User and providing User input to the ECI Client.
5. **ECI Chip Manufacturer（J.1012）:** A company providing systems on a chip that implement ECI specified chipset functionality.
6. **ECI Client (Embedded CI Client) （J.1012）:** The implementation of a CA/DRM client which is compliant with the Embedded CI specifications.

 NOTE – It is the software module in a CPE, which provides all means to receive in a protected manner, and to control the execution of a consumer's entitlements and rights concerning the content that is distributed by a content distributor or operator. It also receives the conditions under which a right or an entitlement can be used by the consumer, and the keys to decrypt the various messages and content.

1. **ECI Client Image（J.1012）:** File with software as VM code, and initialization data required by the **ECI Client Loader**.
2. **ECI Client Loader（J.1012）:** The software module part of the ECI Host, which allows downloading, verifying and installing new ECI Client software in an ECI Container of the ECI Host.
3. **ECI Container （J.1012）:** Asingle VM instance with complementary support libraries and ECI API that permits a single instance of an ECI Client to run on a CPE.
4. **ECI Ecosystem（J.1012）:** A commercial operation consisting of a TA and several platforms and ECI compliant CPEs in the field.
5. **ECI Host（J.1012）:** The hardware and software system of a CPE, which covers ECI related functionalities and has interfaces to an ECI Client.

 NOTE – The ECI Host is one part of the CPE firmware.

1. **ECI Host Image（J.1012）:** File(s) with software and initialization data for an ECI environment

 NOTE 1 – An ECI Host image may consist of a number of ECI Host Image files.

 NOTE 2: – It may also contain other software that does not cause interference with or permit undesirable observation of the ECI Host.

1. **ECI Host Loader（J.1012）:** software module, which allows downloading, verifying and installing ECI Host software into a CPE.

NOTE – In a multi-stage loading configuration this term is used to refer to all security critical loading functions involved in loading the ECI Host.

1. **ECI Root Certificate（J.1012）:** Certificate which issues to verify items approved by an ECI TA
2. **Entity（J.1012）:** organization (e.g., manufacturer, operator or security vendor) or real world item (e.g., ECI Host, Platform Operation or ECI Client) identified by a unique ID in an ECI Ecosystem.
3. **Export Chain（J.1012）:** Chain of certificates used for authorization of export to one or a group of Micro DRM Systems.
4. **Export Connection（J.1012）:** authenticated relation between an ECI Client that can decrypt content and a Micro Server that can re-encrypt content.
5. **Export Group（J.1012）:** Group of Micro DRM-Systems, to which export is permitted
6. Father（J.1012）: Signatory of the Certificate of the Child Entity.

NOTE – **Father, Children, Brother** are referring to entities that manage **Certificates**.

1. **Image Series（J.1012）:** Series of images for an ECI Host or an ECI Client that are different depending on the CPE\_id of the CPE, nevertheless represent (nearly) identical functionality.
2. **Import Chain（J.1012）:** Chain from the POPK of an ECI Client to an Entity that represents an export system or an Export Group.

NOTE – An Export Chain and a matching Import Chain can be used to authenticate a Micro Server session importing content to an exporting ECI Client.

1. **Import Connection（J.1012）:** Approved connection from an ECI Client to a Micro Server that permits it to import decrypted content for subsequent re-encryption.
2. **Manufacturer（J.1012）:** Anentity which develops and sells CPEs, which accommodate an implementation of the ECI system and allows ECI Hosts and ECI Clients to be installed per software download.
3. **Media Handle（J.1012）:** Reference to a single program decryption or re-encryption processing setup between an ECI Client and an ECI Host.
4. **Micro Client（J.1012）:** ECI Client or non-ECI client that can decrypt content which was re-encrypted by a Micro Server.
5. **Micro Server（J.1012）:** ECI Client that can import decrypted content, re-encrypt this content and authenticate a specific ECI Client or group of ECI Clients as the Target for subsequent decryption
6. **Micro DRM System（J.1012）:** Content Protection System that re-encrypts content on a CPE with a Micro Server and that permits decoding of that re-encrypted content by authenticated Micro Clients.

NOTE – Micro Server and Micro Clients being provisioned by a Micro DRM System operator.

1. **Operator（J.1012）:** Organization that provides Platform Operations that is enlisted with the ECI TA for signing the ECI Ecosystem.

NOTE – An Operator may operate multiple Platform Operations.

1. **Platform Operation (PO) （J.1012）:** specific instance of a technical service delivery operation having a single ECI identity with respect to security
2. **Re-encryption Session（J.1012）:** A process controlled by a Micro Server of importing content from an Import Connection, re‑encrypting it and producing the decryption information necessary by the authenticated Target to subsequently decrypt it.
3. **Request（J.1012）:** A message from a sender to a receiver asking for certain information or to perform certain operation within an ECI Ecosystem, which is specified in the data fields of that request.
4. **Response（J.1012）:** A message within an ECI Ecosystem answering a request.
5. **Revocation List (RL) （J.1012）:** A list of Certificates that have been revoked and therefore should no longer be used.
6. **Root（J.1012）:** A public key or Certificate containing a public key that serves as the basis for authenticating a chain of Certificates.
7. **Secure Authenticated Channel (SAC) （J.1012）:** A communication path (channel) that has been established between two Entities where the Entities have securely identified themselves to each other (authenticated) and agreed on an encryption of data transferred between them (secure).
8. **Sender Public Key (SPK) （J.1012）:** The public key of the sender of the encrypted content used in an ECI Ecosystem to verify the origin of the signature of the first key of a key chain used to decrypt the content, the sender being part of a Platform Operation.
9. **Smart Card:** A detachable hardware security device used by several CA or DRM providers to enhance the level of security of their products in an ECI Ecosystem.
10. **Target（J.1012）:** Micro Client or a group of Micro Clients for which content is re‑encrypted by a Micro Server.
11. **Trust Authority (TA) （J.1012）:** An organization governing all rules and regulations that apply to a certain implementation of ECI and targetted at a certain market.

 NOTE – The Trust Authority has to be a legal entity to be able to achieve legal claims. The Trust Authority needs to be impartial to all players in the ECI Ecosystem that it is governing.

1. **Trusted Third Party (TTP) （J.1012）:** Security services provider, which issues Certificates and keys to compliant Manufacturers of the relevant components of an ECI-system

NOTE– It is under the control of the Trust Authority (TA).

1. **User（J.1012）:** A person who operates an ECI compliant device.
2. **VM Instance（J.1012）:** Instantiation of VM established by an ECI Host that appears to an ECI Client as an execution environment tooperate in.
3. **Bytecode（J.1013）:** Code of **ECI Client** (typically comprising a Conditional Access kernel or Digital Rights Management client) that is executed by the VM.
4. **Native Code（J.1013）:** programmatic code written in the native executable instruction set of the **ECI Host** processor.
5. **AS-API（J.1014）:** Application programming interface between the ECI Client and its ECI Host permitting the ECI Client to exchange information with and perform operations on its AS Slot.
6. **Authentication Mechanism（J.1014）:** Key Ladder Block function as defined in [ITU-T J.1015] that permits an AS Slot to provide secure key applications for purposes other than content decryption and encryption, like authentication.
7. **Content Properties (CP)（J.1014）:** Properties of the content that provide information on rights and obligations associated with subsequent applications or transformations of the content, such as usage rights information, selective output control and parental control information.
8. **Key Ladder（J.1014）:** Function of the Key Ladder Block as defined in [ITU-T J.1015] for computing control words and associated control word usage information for application in the content decryption or re-encryption function of a CPE.
9. **Key Ladder Block（J.1014）:** Robust secure mechanism to compute decryption, encryption and authentication keys as defined in [ITU-T J.1015], both Key Ladder and Authentication Mechanism.
10. **Provisioning Server（J.1014）:** Server, typically located in a secure back office location, that provisions keys and other secure information to facilitate an encryption or decryption function through an AS Slot.
11. **Robustness（J.1014）:** Property of the implementation of a specified ECI secure function representing the effort and/or cost involved to compromise the security of the implemented secure function.
12. **Secure Video Path（J.1014）:** all CPE functions performing processing on content (and temporary storage required thereto) from and including Content Decryption through and including content re-encryption by means of a Micro Client or Output Protection System.
13. **Security Vendor（J.1014）:** Company providing ECI security systems including ECI Clients for Operators of Platform Operations.
14. **certification authority (J.1015):** party that is responsible for managing public-key certificates in an embedded common interface (ECI) ecosystem. A certification authority is trusted by all other parties in the system to perform operations associated with certificates.
15. **chipset-ID (J.1015):** Non-secret number that is used to identify a chipset within an ECI ecosystem.
16. **content protection system (J.1015):** System in an ECI ecosystem that employs cryptographic techniques to manage access to content and services. The term may be interchanged frequently with the alternate Service Protection system. Typical systems of this sort are either conditional access (CA) systems or digital rights management (DRM) systems.
17. **content provider (J.1015):** party that distributes digital content to a content receiver in an ECI ecosystem.
18. **content receiver (J.1015):** device that is used to access digital content within an ECI ecosystem. A content receiver contains a chipset with a content descrambler.
19. **content descrambler (J.1015)**: component in the chipset of an ECI ecosystem that is capable of decrypting content. A content descrambler may also be capable of encrypting content (for the purpose of content re‑encryption). In this Recommendation content encryption/decryption uses a symmetric encryption scheme. For MPEG-2 content, content encryption and decryption are also referred to as scrambling and descrambling, respectively.
20. **control word (J.1015)**: secret key used to encrypt and decrypt content within an ECI ecosystem. In digital rights management systems, a control word is typically referred to as a content key.
21. **cryptographic hash function (J.1015):** unkeyed cryptographic function in an ECI ecosystem that takes data of arbitrary size, referred to as the message, as input and produces an output data block of fixed size, referred to as the message digest. Assumed properties of the **cryptographic hash function** in this Recommendation are that the cryptographic hash function behaves as a random function and is second preimage resistant.
22. **digital signature scheme (J.1015):** keyed asymmetric cryptographic scheme that is used to protect the authenticity of data in an ECI ecosystem. A digital signature scheme consists of a key generation algorithm, a signature generation operation and a signature verification operation. Keys are generated as (secret/private key, public key) pairs. The data is signed using a secret/private key and the corresponding public key is used to verify the signature. The digital signature scheme specified in this Recommendation is used to protect the authenticity of messages as defined in [b-ROEL]; in particular, the scheme is not used to provide non-repudiation or source authentication in this Recommendation.
23. **ECI ecosystem (J.1015):** A commercial operation consisting of a trust authority and several platforms and ECI - compliant customer premises equipment in the field.
24. **message authentication code algorithm (J.1015):** keyed symmetric cryptographic algorithm that is used to protect the authenticity of data in an ECI ecosystem. A message authentication code algorithm takes a message and a secret key as inputs, and produces an output data block referred to as the MAC. The message authentication code algorithm as specified in this Recommendation is used to cryptographically bind a ciphertext message to its associated data; in particular, the algorithm is not used to provide source authentication in this Recommendation.
25. **public-key encryption scheme (J.1015):** keyed asymmetric cryptographic scheme that is used to protect the confidentiality of data in an ECI ecosystem. A public-key encryption scheme consists of a key generation algorithm, an encryption operation and a decryption operation. Keys are generated as (public key, secret/private key) pairs. Data is encrypted using a public key and the data is recovered from the ciphertext using the corresponding secret/private key.
26. **symmetric encryption scheme (J.1015):** keyed symmetric cryptographic scheme that is used to protect the confidentiality of data in an ECI ecosystem. A symmetric encryption scheme consists of a key generation algorithm, an encryption operation and a decryption operation. The encryption and decryption operations of a symmetric encryption scheme use the same secret key as input.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_