INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG9–R17-ANNEX 1

STUDY GROUP 9

Original: English

Question(s): All/9 May 2020

ANNEX 1

Source: ITU-T Study Group 9 (Television and sound transmission and integrated broadband cable networks)

Title: ANNEX 1 to Report SG9-R17 on "Summary of discussion points on Embedded Common Interface (ECI)

Purpose: Information

Contact: TSB Tel: +41 22 730 5858
Fax: +41 22 730 5853
Email tsbsg9@itu.int

Keywords: ITU-T SG9; Report 17 ANNEX 1, ECI

Abstract: This is Annex 1 to the meeting report (SG9-R17) of the fifth Study Group 9 meeting, which was held fully virtual, 16-23 April 2020, during the study period 2017-2020. This document is referenced by five ITU-T Recommendations, namely ITU-T J.1012, J.1013, J.1014, J.1015 and J.1015.1 and is made publicly available by the ITU on request of ITU-T Study Group 9.

ANNEX 1 to Report [R17]

(SG9 Meeting, fully virtual, 16-23 April 2020)

Summary of discussion points on Embedded Common Interface (ECI)

Introduction

These discussion points were raised in Contributions submitted to the ITU-T Study Group 9 meeting (16-23 April 2020) from ITU-T Member States Israel and Australia, ITU-T Sector Member Samsung, and SG9 Associates Sky Group and MovieLabs, who proposed that a number of changes be included in the ECI-related Recommendations (ITU-T J.1012, J.1013, J.1014, J.1015 and J.1015.1), but agreement was not reached with other ITU-T Members who provided a feedback on each of the concerns raised. This document is made publicly available by the ITU on request of ITU-T Study Group 9.

Table of Contents

1. Overview table

This table attempts to present all the points made during this meeting of ITU-T Study Group 9 (SG9), in what contribution they can be originally found (with page number in the contribution), and what rationale was given for not accepting them.

	Israel C-0122	**Australia C-0121**	**Samsung C-0143**	**Sky C-0146**	**MovieLabs C-0147**
ECI is too complex	Page 2	Page 1	Page 1-2	Page 4	
Remove DRM or use existing commercial DRM	Page 2		Page 2	Page 4	Page 8
Don't allow re-encryption				Page 4	
Remove SW management	Page 2				
Add secure storage & client crypto					Pages 2-7
Make secure storage/crypto mandatory & HW-based	Page 2				
Allow vendor-specific key ladders	Page 1				
Use J.1207's TEE requirements	Page 1				
Include TEE implementation spec for VM			Page 1		
Use stronger hash			Page 1		
Use x.509 certs			Page 2		
Define testing/verif			Page 2		
Comms between clients				Page 3	
ETSI liaison/review					Page 8
Peer-review				Page 5	
Remove the TA		Page 1-2			
Set C&R rules & define TA	Page 2		Page 3	Page 4	Page 7
Diversity in ECI hosts & clients				Page 3	
Runtime integrity checking				Page 3	

2. Summary of each concern

2.1. General concern: ECI is too complex

To be found in the following contributions

Australia (C0121) page 1

Israel (C0122), page 2

Samsung (C0143), page 1-2

Sky (C-0146), page 4

What is the concern?

Significant efforts must be made to reduce the complexity of the proposed specifications before ECI is adopted.

What is its rationale?

ECI's excessive complexity and untested status would be a burden to implementers – CAS vendors, device manufacturers and service providers – and a security risk for consumers and content providers.

It is an axiom of security that its worst enemy is complexity, and yet the specification, which runs to over 500 pages, is arguably the most complex CAS/DRM system ever designed. This problem is compounded the fact that, while most systems have been implemented, tested and refined before they are standardized, ECI has never been implemented, instead pushing the burden of debugging the specification onto the manufacturers of ECI-compliant devices, CAS vendors and service providers. The overly large and complex specification opens up more attack planes, makes testing impractical and restricts innovation by security vendors.

The impact of ECI's complexity on silicon is of particular concern. Samsung has its own SoC division, which has investigated the likely impact of this specification on its silicon. Their conclusion is that, compared to current implementations, the hardware and software complexity will increase the costs of the security silicon area, with no identified benefit to device manufacturers. In particular, the concern that the requirements for hardware control of an 'inter' crypto engine, specifically where the AES output shall be control by hardware when transferred to RSA, SHA and vice versa will be complex and add significant cost. Sky also said that the SoC solutions currently in the market do not cater for ECI and development of a new larger SoC could be prohibitively expensive.

Australia also made the point that the cryptography is too complex to be implemented in hardware (unlike with other CAS systems), so device makers will have to add an additional security processor to implement the specified cryptography.

Statement of ECI Editors

The statement of complexity is a very general one. The comparison with the developments within the CI+ project show that complexity and additional cost is not a relevant argument as CI+ has been successfully established in the market. It is assumed that the processing power of state-of-the-art chipsets will be able to handle the processing requirements of ECI.

2.2. Remove Digital Rights Management (DRM) or leverage existing commercial DRM solutions

To be found in the following contributions

MovieLabs (C0147), page 8

Samsung (C0143), page 2

Israel (C0122), page 2

Sky (C0146), page 4

What is the concern?

Remove DRM from the scope of the requirements and architecture Recommendations (J.1010 and J.1011) or leverage existing commercial DRM solutions rather than create a set of DRM specs.

What is its rationale?

ECI tries to do too many things at once: broadcast CAS and online DRM/in-home distribution. Traditional broadcast services and internet services have very different technical needs. Broadcast delivery benefits from standardization because there is only one broadcast signal that is received by all devices for both the content (video) and content protection (CAS). But with internet delivery, the two are completely separable. In fact, DRM already has well-proven market solutions: it is an easy and common practice for the service provider to stand up DRM servers that support every commercially relevant DRM system to protect the content. Including DRM in ECI therefore proposes a solution that is technically complex and potentially insecure to a problem that doesn't exist for consumers, for device makers or for service providers.

However, if we cannot remove DRM from the requirements of ECI, we should at least reconsider why ECI doesn't leverage existing commercial solutions. Why reinvent the wheel? Why create what will be an inferior, poorly supported and soon to be obsolete solution when existing widely-used, proven and innovative commercial solutions exist?

Statement of ECI Editors

DRM is an essential part of the approved ECI requirements

2.3. Do not allow re-encryption

To be found in the following contribution

Sky (C146), page 4

What is the concern?

ECI should not allow re-encryption.

What is its rationale?

Re-encryption is not required by the market, and in any case, most content rights agreements preclude export.

Statement of ECI Editors

Re-encryption is clearly defined in the ECI specifications because an ECI Client is only able to implement content re-encryption if an appropriate API is available to control related functions in the ECI Host. This does not exclude solutions where content export is prohibited.

2.4. Remove software management

To be found in the following contribution(s)

Israel (C0122), page 2

What is the concern?

Remove software management

What is its rationale?

This would help avoid some of ECI's complexity.

Statement of ECI Editors

Software management is an essential part of the draft ECI specification

2.5. Add secure storage & client crypto

To be found in the following contributions

MovieLabs (C0147), page 2-7

What is the concern?

APIs should be added to J.1012 to support:

- secure storage;
- memory-to-memory encryption; and
- crypto library APIs.

What is its rationale?

These features are commonly offered by current commercial CAS and DRM systems. Without them, ECI would not offer an environment suitable for high-quality competitive commercial multimedia services. For example, it's important to understand that the use cases that require secure storage – such as to store DRM-related private asymmetric keys, DRM license files, and DVR content recorded by a 1-way CAS client – are

not theoretical scenarios but rather essential for modern TV services. Service providers will demand that CAS vendors support these features.

It's also important to note that these features are included in the requirements of other relevant existing or proposed standards:

– GlobalPlatform includes explicit requirements for secure storage and crypto library APIs. That is highly relevant because ECI requires the use of a Trusted Execution Environment (TEE), which has been standardized for use in mobile devices, STBs, smart TVs and other devices by GlobalPlatform.

– There are also two proposed ITU specifications that include explicit requirements for secure storage, memory to memory encryption and crypto library APIs efforts: Downloadable conditional access system (DCAS) for unidirectional networks (J.1026, 1027 and 1028); and DCAS for bidirectional network (J. twoway-dcas-part1, part2 and part3).

The fact that current commercial CAS and DRM systems require these features and that they are supported by both existing standards and other proposed ITU standards means that, without them, the current ECI specifications do not meet their own requirement (specified in Section 6.2 of J.1010) to "provide Enhanced Security features comparable to those available with today's state of the art CA/DRM Systems."

Statement of ECI Editors

Secure time, a random generator and encryption functionalities are defined in the draft specification. In case this does not fully meet future content protection requirements, these functionalities have to be dealt with a new work item.

2.6. Mandatory, hardware-based secure storage/crypto

To be found in the following contribution

Israel (C-0122) page 2

What is the concern?

The secure execution environment should be modified as follows:

– Secure storage should be mandatory.

– Secure storage should be hardware-based.

– The secure execution environment should allow CAS vendors to implement the cryptographic infrastructure they need.

What is its rationale?

Along with a secure execution environment, the DCAS architecture documents also refer to secure storage. For example section 6.2.3.2 of J.1027 states: "When storing critical data, one-way DCAS client software shall use the secure storage function provided by HSM via SAC."

By contrast, the ECI spec (J.1012, section 10) says that many of the features such as secure clock or secure files system are optional. They are optional even in smart card-based systems that depend on such security.

Statement of ECI Editors

A random generator and encryption functionalities are defined in the draft specification which can be used to implement secure storage. In case this does not fully meet future content protection requirements, these functionalities have to be dealt with a new work item.

2.7. Allow vendor-specific key ladders

To be found in the following contribution

Israel (C-0122), page 1

What is the concern?

Allow a key ladder per vendor.

What is its rationale?

ECI (specifically Section 7 of TD-GEN-0502-J.1015) only provides one common key ladder for all CAS vendors. The spec should allow a key ladder per vendor. This would allow greater security because each vendor would be isolated from breaches that might compromise other vendors. It would also provide room for innovation. In the consultation paper on STB interoperability that it published last November, India's telecom regulator (TRAI) similarly explains the benefits of having one key ladder per vendor.

Statement of ECI Editors

The ECI key ladder is an essential part of the approved ECI requirements, enabling the swappability of ECI Clients in ECI-compliant devices.

2.8. Use J.1027's TEE requirements

To be found in the following contribution

Israel (C-0122) page 1

What is the concern?

The execution requirements of the proposed unidirectional DCAS specification J.1027 (specifically section 6.2.3.3) should be made mandatory in ECI.

What is its rationale?

All CAS vendors need the environment that handles the keys and decrypts the video to be secure. This is critical to secure the business of the operator.

Statement of ECI Editors

Basic functionalities have been specified in new clause 6.2 of J.1014. Further detailed specifications have to be defined by the Trust Authority of a future ECI eco-system.

2.9. Include TEE implementation spec for the VM

To be found in the following contribution

Samsung (C0143), page 1

What is the concern?

ECI should include a TEE implementation specification for the VM.

What is its rationale?

It is important to ensure consistent and robust implementation. However, some classes of device may not be able to implement a VM inside the Trust zone, which would either compromise security significantly or exclude some classes of device from accessing some content.

Statement of ECI Editors

Basic functionalities have been specified in new clause 6.2 of J.1014. Further detailed specifications have to be defined by the Trust Authority of a future ECI eco-system.

2.10. Use stronger hash algorithms

To be found in the following contribution(s)

Samsung (C0143) page 1

What is the concern?

SHA384 or SHA512 should be required.

What is its rationale?

This specification will, if approved in its current form, still take several years before it is common place in the market. There is a concern about the requirements for the HASH algorithm. For longevity beyond 2025, one would expect to see SHA384 or SHA512 be required.

Statement of ECI Editors

As SHA 384 or SHA 512 might be relevant for new implementations earliest by 2025, ECI editors decided to stick with the SHA256 algorithm. A future update would be a minor change in a revision of the specification.

2.11. Use x.509 certificates

To be found in the following contribution

Samsung (C0143), page 2

What is the concern?

ECI should use x.509 certificates.

What is its rationale?

ITU-T X.509 certificates are an existing standard that is used around the world, and ITU-T is rightly proud of having developed this standard. Using it in ECI would simplify the architecture and allow the use of OpenSSL library to check content and to more easily handle the source as well as in the script.

Statement of ECI Editors

The ECI solution has the advantage of less complexity and therefore provides higher efficiency.

2.12. Testing and verification is not fully defined

To be found in the following contribution

Samsung (C-0143), page 2

What is the concern?

Any published specification should include a cross-industry agreed test and verification requirement.

What is its rationale?

Any new function or feature must have a well-defined test and verification process before it can be implemented to avoid the risk of expensive to rectify issues being identified in the field.

Any published specification should include a cross-industry agreed test and verification requirement to ensure that implementations are consistent on a global level and not left to individual administrations who may not be experts to decide.

Statement of ECI Editors

Testing and verification shall be subject of further specification work of the Trust Authority of a future ECI eco-system.

2.13. Communication between ECI clients

To be found in the following contribution

Sky (C0146), page 3

What is the concern?

Do not allow communication between ECI clients.

What is its rationale?

Communication between ECI clients creates a security risk because a malicious ECI client could attack another. The logistical problem it generates is an exponential burden to interoperability testing as the number of possible ECI clients increases.

Statement of ECI Editors

The client-to-client communication of the ECI system is a feature which is available to any client. However, the client decides whether it can trust another client to open a communication channel.

2.14. ETSI should review ECI

To be found in the following contributions

MovieLabs (C0147), page 8

Oral intervention by UK administration

What is the concern?

ETSI should review ECI before final SG9 approval.

What is its rationale?

The ITU and ETSI have a history of cooperation on standards, which has been guided by an MoU since 2000 (renewed in 2012 and 2016: https://www.itu.int/en/ITU-T/extcoop/Documents/mou/MoU-ETSI-ITU-201605.pdf) The proposed ECI specifications are derived from a set of ETSI specifications.

ITU should consult ETSI, including via an exchange of liaisons, on the following points before it finally adopts ECI:

– Section 4.3 of the MoU expressly directs ITU and ETSI technical groups to develop and follow an effective process of consultation and harmonization before final approval. Section 2.1 of the MoU provides that an iterative process should be followed, by which an initial ETSI proposal to ITU is reworked by ETSI on the basis of comments and proposals made in ITU meetings. However, the last liaison to ETSI regarding ECI (SG9-LS49) was made in January 2018: it reflects neither the subsequent significant normative changes made to the draft Recommendations nor the subsequent change in document structure of ITU-T J.1015 (from which ITU-T J.1015.1 was split).
– To harmonize ETSI and ITU standards, the last sentence of section 4.2 of the MoU expresses a clear preference for incorporation by reference. Instead, the proposed ECI Recommendations directly incorporate text from the ETSI specifications.
– Significant portions of some of the proposed ECI specifications have been copied from ETSI specifications, which are copyrighted by ETSI. However, it is not clear that the ITU has obtained license or some other legal right to use this copyrighted text. The ITU must ensure it does so before approving ECI.

Statement of ECI Editors

During development of the ISG ECI Group specifications the liaison with ITU-T SG9 (Q2/9) was communicated within ETSI and reported in each of the ECI meeting reports. Additional liaisons from ITU-T SG9 to ETSI may be sent after TAP approval.

2.15. ECI should be peer-reviewed

To be found in the following contribution

Sky (C-146) page 5

What is the concern?

ITU should require ECI to undergo independent peer review by a competent, professional body before giving it further consideration.

What is its rationale?

Given the breadth and gravity of concerns expressed and the fact that they are shared by a large and growing swath of stakeholders, ECI needs to be thoroughly reviewed by independent experts.

Statement of ECI Editors

The ECI specs have been submitted to ITU-T SG9 in summer 2017. The ITU experts have worked 2 and a half years with increasing international participation reviewing and extending this set of specifications. ECI experts consider this as the best possible peer review.

2.16. Remove the TA

To be found in the following contribution

Australia (C0121) page 1-2

What is the concern?

There should not be a trust authority: instead, ECI should explicitly provide that compliance and enforcement are collaboratively administered by the service provider, CAS vendor and/or DRM provider and device manufacturer.

What is its rationale?

The draft ECI specification shifts compliance responsibilities (which for DRM or CAS are normally collaboratively administered by the service provider, CAS/DRM provider and device manufacturer) to a "trust authority," making it difficult to test compliance, to quickly access needed information, and to fix data breaches. This is a structural and conceptual flaw.

Doing away with the TA would also require that ECI not be published until comparable specifications are completed on technical compliance and robustness rules.

Statement of ECI Editors

The Trust Authority is an essential part of the approved ECI requirements

2.17. Set C&R rules and define the TA

To be found in the following contributions

MovieLabs (C0147), page 7

Israel (C0122), page 2

Samsung (C0143), page 3

Sky (C-0146) page 4

What is the concern?

Don't publish the technical Recommendations until comparable Recommendations are completed on technical compliance and robustness rules and on the creation and operation of Trust Authorities.

What is its rationale?

Viable content protection ecosystems require much more than technology. Functional technical specifications are not separable from the technical compliance and robustness specifications or from the administrative aspects of establishing a Trust Authority (TA). A TA defines the legal framework under which the technical system is deployed. This includes referencing a set of Compliance & Robustness Rules that more fully define the secure end-to-end implementation of the technical specifications, device and operator certification, breach response and revocation procedures. These legal frameworks define the rights and roles of the various participants in the ecosystem, including device makers, service operators, testing entities and content providers. The success of ECI in the marketplace vitally depends on CAS vendors, service providers and content owners trusting the TA.

Piracy on the ECI platform would be totally out of the platform operator’s control. The impact of such piracy would be a migration of customers to the ECI platform with a consequent loss of revenue to the platform operator. This raises questions about who is liable and who will pay compensation?

One particular issue about the TA is important: will there be several TAs (e.g. one per country or region), or will there be a single, global, market-accepted TA? Samsung in particular would strongly prefer the latter. Either way, that is an important issue and if there are going to be several TAs there needs to be at a minimum greater coherence, and ideally uniformity, between them in the C&R rules they will enforce, to avoid market fragmentation that would inhibit support from device manufacturers, take-up by service providers and trust on the part of content owners.

It is a regrettable omission from the ECI specification to not fully address this as is done by alternative solutions such as CI+.

Statement of ECI Editors

This activity is subject to the Trust Authority of a future ECI eco-system.

2.18. Allow greater diversity in ECI hosts and clients.

To be found in the following contribution

Sky (C-0146) page 3

What is the concern?

Insufficient diversity in ECI hosts and clients.

What is its rationale?

Diversity allowed in ECI hosts and ECI clients is too limited to allow for sufficient differentiation to support the best practice “Hack one, hack only one” – which is a requirement for compliance with MovieLabs ECP v1.2.

Statement of ECI Editors

Best practice “Hack one, hack only one” is available as any ECI-compliant device possesses a securely protected unique key.

2.19. Require runtime integrity checking

To be found in the following contribution

Sky (C-0146) page 3-4

What is the concern?

No integrity checking is performed during runtime.

What is its rationale?

This means that a hack made after boot up would not be detected. MovieLabs ECP v1.2 requires runtime integrity checking.

Statement of ECI Editors

This feature is possible for any ECI Host or Client and therefore dependent on the individual implementation. The Trust Authority of a future ECI eco-system may have further detailed requirements on this topic.

_____