1 Cisco’s comments regarding the TRAI/C-Dot proposal

> **Note**
>
> The comments below are based on the Consultation Note on Solution Architecture for Technical Interoperable Set Top Box dated 11/08/17 describing the proposed system. Many of the details are still unclear, therefore some assumptions are made.

1.1 Security

1.1.1 SoC

The primary weakness in the proposed system is on the SoC side. Recent years have seen hackers focus their efforts on attacking the SoC and in fact multiple instances of poor security implementations in “standard” SoC hardware have led to wide spread hacks on Service Providers. As a result, today’s CA systems depend on advanced, proprietary security modules incorporated into the SoC hardware to provide Service Providers with sufficient levels of security.

This is not just a matter of “security by obscurity”. The proprietary hardware in the SoC is produced by the CA providers and has undergone rigorous testing and QA procedures throughout the design and implementation. The resulting HW blocks provide a notably higher level of security than a standard cryptography block developed and implemented by the SoC vendor.

The CA proprietary HW implemented in the SoC is of such a high level of security, that many Service Providers are moving towards deploying a CA system based solely on this HW block, without a smart card. This process will result in lower STB costs, and ultimately keep consumer costs down as well.

The proposal, as-is, represents a step-backwards in the level of security currently deployed by Service Providers: A secure channel is negotiated by the STB software, and then the CW is passed from the smart card to the SoC protected by the secure channel where it is then decrypted and passed to the descrambler. In such a scheme, it is critical to maintain the security of the SoC’s private key as well as the volatile session key used for encrypting the CW. Historically, pirates have focused on the SoC as a weak point from which to extract the CW and illegally share it.

In our experience, the mechanism used for encrypting the CW must be designed and implemented exceptionally carefully. STB software can almost always be compromised and thus all elements on the critical path of CW protection must be implemented in pure hardware. In this case, it seems likely this would imply that the vast majority of the secure channel logic would need to be implemented in such software, a significant challenge and a major risk. The current proposal indicates that significant portions of the key material would reside in STB RAM at some point, exposing the system to significant hacking.

The dependence on asymmetric cryptography and certificates on the critical path of this scheme is particularly worrisome, as private key operations have proven to be particularly susceptible to various side channel attacks over the years. If even one private key is leaked, the system is essentially broken. One can try to revoke a compromised key, but years of industry experience have shown that wide-scale revocation rarely possible in an open system, particularly a system with such limited two-way communications.

Furthermore, the private keys must be secured not just while in use, but throughout their entire life-cycle from the STB manufacturers' facilities and also while at-rest in the STB in the field. Historically, the STB manufacturers have not been responsible for safeguarding these system-level secrets and it is unclear that they have the facilities and knowledge required to design and implement such systems.

Furthermore, the proposal discusses security requirements vaguely. For example on Page 22 the document states:, "Such data must be directly given as input to the necessary hardware/secure processor and should not be accessible to any other software or hardware module outside SOC.". What kind of protection is required for those secrets? Are there permitted or approved schemes for that protection?

1.1.2 Countermeasures

Another important aspect is counter-measures. In a well-designed system, counter-measures are an integral part of the end-to-end solution, usually implemented by the CA HW modules (SoC and/or smart-card) and are intended to be used against various attacks on a service provider. However, the proposed architecture limits the counter-measures that can be used:

- Many of these counter-measures depend on system-wide deployment and thus the inclusion of devices that do not support these counter-measures, prevents the CA providers from deploying their most effective weapons in the fight against piracy
- Some of the counter-measures, are based on detecting differences between the legal devices and illegal ones. Having a global, standardized and publicly known requirements for the STB functionality will make it easier for the attacker to implement a similar functionality in an illegal device, or hack the legal device in order to attack the system; in both cases, most of the countermeasures will fail to identify the illegitimate usage.

1.2 Functionality

Another important aspect of the proposed system is that it will require significant changes in multiple fronts:

- Card/STB CA SW (Verifier) API: impacts both Headend and Client system components
- STB-Card-Mobile# coupling proposed in the CA system for every subscriber: impacts the control plane and back office services, including the 3rd-party Subscribers Management System
- New EMM structure to support portioning to Group IDs: in addition to the impact on the CA components (HE, Client and Smartcard) this could result with an **impact on the EMM bandwidth**
- Maintenance & delivery of CA certificates for smartcard and STB: significant operational impact

1.3 UHD

The studios have produced many licensing requirements for Ultra HD (4K) content. (For example: "MovieLabs Specification for Enhanced Content Protection"). This proposal does not address those requirements. Some examples: the ability of the CA system to verify that the STB has the latest SW version and forensic watermarking.

Additionally UHD licensing requirements require the operator to validate trusted execution environments, STB compliance, etc. How can an operator meet these requirements if they have no visibility into STB HW and SW?

1.4 Breach Responsibility

Currently a CA operator takes complete breach responsibility for the system. If any component in the system is hacked the operator has one business entity to turn to, to address the breach. There are often significant financial penalties to Conditional Access vendors for security failures. With this proposal there is no entity that is responsible for security. If a specific SoC or MW is hacked, the CA vendor or operator has no way to address the breach.

1.5 Middleware

As per the proposal a middleware is to be developed against a common specification or platform. The middleware could then be developed by middleware vendors or by STB manufacturers.

However, for a 3rd party to develop middleware - which can be downloaded to any manufacturer's device within an operator's network, there also needs to be a standardized hardware and software environment specified. Such specification in other countries, has significantly increased the cost of hardware (ex, DAVIC).

Even with open middleware specifications such as MHP or OCAP, the middleware is directly ported onto the hardware. Upgrading a middleware to any hardware with an independent porting layer could be very challenging. Existing middleware vendors who are able to run on multiple hardware platforms, have achieved this using well defined hardware interface porting layers owned by them. Even those middleware do not support run time validation, or support download onto any generic STB. This implies there is a need for per operator certification and testing of the middleware software, against each hardware type, which is a tremendous exercise.

Advanced middleware functionalities such as PVR would need further development of specifications to ensure proper content security and rights handling.

Furthermore, within an operator's environment, if multiple manufacturer enabled middleware are to used, then based on each platform's capability and performance, there can be a very inconsistent user experience that can lead to consumer frustration.

Common Runtime for applications: For creating value added services, it is proposed that the operators use downloadable applications. These application do need a common runtime to be available across all manufacturers. However without the verification mechanism to certify and classify the runtimes based on the device/porting capability it will be extremely difficult to achieve the ability to run these applications on any manufacturer device.

1.6 EPG

The proposal suggests two models of EPGs.

Simple EPGs which are not operator specific and downloadable operator specific EPGs.

Simple EPG could offer simple channel change experience with minimal content discovery. This will have limitations even on basic functionalities such as finger-printing, OPPV, broadcast mail/messaging etc. and this requires extensions in the framework.

Advanced EPGs which can be operator specific and which can be downloaded to any manufacturer's device, would require an advanced middleware specification similar to MHP/OCAP. The experience in MHP and OCAP have proved that even applications developed against these specifications require hardware specific integration and long validation cycles. This is because the performance/stability can be highly dependent on the specific hardware and platform driver capability.

1.7 Software upgrade

Unlike mobiles, which receive software upgrade from manufacturers via a connected environment, the satellite/cable devices need to receive an upgrade from their respective operator's broadcast network, to which they are tuned to.

If any STB sold in India must work under any operator then the operators will have to support the ability to carry the upgrade images of ALL and ANY new such devices manufactured for India. The maintenance and management of new images due to new features added or bug fixes found can be extremely significant.

The above issues could be partially resolved by providing an ability to upgrade through internet or by USB memory based upgrades. However, this could mean an inability to bypass upgrade of the right software version required to deliver a new service, or removal of an older version which might have got compromised.

1.8 Broadcast system: Operator Services and signaling

The system proposes to use standard DVB signaling of services and metadata. Indian TV eco system has grown with specific needs which require extensions to DVB for offering acceptable end customer experience w.r.t. discovering content as well ability to support multiple languages in a scalable way.

An additional comprehensive new specification is to support the current content discovery experience.

The following table gives a sample list of features which require extensions to offer the experience required in India.

Feature	Details	DVB areas which would need extensions
Service Filtering	Indian satellite/cable operators have a large list of channels which needs to be filtered in EPG for a better content discovery	SDT, BAT. The DVB definition of content descriptor does not satisfy simple India scenarios such as filtering channels for respective region's interest.
Pay per view events	Enabling of pay per view events purchasable over phone call/sms	Event information tables
Software update signalling	Availability of software (CA, Middleware, drivers, OS, EPG/system application) signalling of all manufacturers and the new software itself to be kept for download	DVB SSU needs to be extended to cover the wide variety of devices and software components.
Multiple languages	Linguistic diversity in India requires numerous languages to be supported; the EIT specification needs to be extended to support compression so that bandwidth utilization will be optimal	EIT
Applications	Applications signalling need to support hardware, device model, operator, middleware version, EPG version addressability	SDT & DSM_CC, AIT
Targeting capabilities	For staged software downloads, targeted value-added services and messages, there is a	New

	need for having a broadcast mechanism which can target the users.	
Controlling feature capability per user	Operators do wish to have control on features per subscriber (e.g. PVR).	New

Building such extensions and getting them supported by operators, manufacturers, software vendors and broadcast system vendors needs significant time and resources to standardize and certify.

1.9 Host Resources

For example, the only host resource defined is for setting filters. Showing OSDs, using STB memory, interactions with a recording system, etc. are not defined. A workable standard will have to have all these resources defined.

1.10 Proposal Maturity

The proposal at this point is a technical direction. It will need to undergo far more detail to make it implementable or verifiable.

1.11 Compliance and Robustness Rules

The document does not discuss which entity is responsible for compliance and robustness or what those compliance and robustness rules are. Nor is the legal framework for producing things compliance with the proposal defined. It is assumed that there will be some standardizing agency to turn the proposal into an actual standard with legal frameworks.

1.12 Certification & Test Suites

An interoperable system by definition requires that independent entities be able to produce their part of the system and to trust that all the other entities have produced their part in compliance with the standard.

For this proposal it means that SoC manufacturers, STB manufacturers, MW vendors, Security Vendors, Video Service Providers, regulatory agencies, and most importantly consumers must trust that each part of the system has been sufficiently designed and verified so that the system works in the real world. If a particular feature or operation does not work in a particular operator network, the consumer has nowhere to turn. Each vendor will blame the other in the ecosystem for non-compliance.

Therefore each part of the system must have a compliance verification suite defined. In addition to a full integrations test suite, the regulatory body must make provisions for each part of the system to be certified for compliance before that system is allowed to be distributed.

At present the TRAI proposal does not discuss certification or a test suite definition.