Телеком Србија
Предузеће за телекомуникације а.д.

Београд, Таковска бр. 2.

ДЕЛОВОДНИ БРОЈ: 419493/1-2023
ДАТУМ: 29.9.2023
ИНТЕРНИ БРОЈ:
БРОЈ ИЗ ЛКРМ:
КАБИНЕТ ГЕНЕРАЛНОГ ДИРЕКТОРА

РЕПУБЛИКА СРБИЈА

РЕГУЛАТОРНО ТЕЛО
ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

ПАК 106306 11103 Београд
Палмотићева бр.2

ПРЕДМЕТ: Достављање коментара на Нацрт правилника о захтевима за интероперабилност аутомобилских радио-пријемника и потрошачке дигиталне телевизијске опреме

Дана 4. септембра 2023. године Регулаторно тело за електронске комуникације и поштанске услуге на званичној Интернет страници објавило је позив стручној и широј јавности, да у оквиру јавних консултација изнесе своја мишљења у вези са Нацртом правилника о захтевима за интероперабилност аутомобилских радио-пријемника и потрошачке дигиталне телевизијске опреме. У складу са наведеним позивом, Предузеће за телекомуникације „Телеком Србија" а.д. Београд, благовремено износи следеће коментаре:

Релевантни члан:

Члан 3. став 1. тачка 1)

„Сва потрошачка опрема намењена за пријем дигиталних телевизијских сигнала (путем кабловске, сателитске и терестричке радиодифузне мреже), која се испоручује на тржишту, продаје или изнајмљује у Републици Србији и која може да дескремблује дигиталне телевизијске сигнале, мора да има следеће карактеристике:

1) дескрембловање дигиталних телевизијских сигнала у складу са јединственим европским алгоритмом за скрембловање (Common Scrammbling Algorithm - CSA) којим управља ETSI.."

Предлог измене:

„Сва потрошачка опрема намењена за пријем дигиталних телевизијских сигнала (путем кабловске, сателитске и терестричке радиодифузне мреже), која се испоручује на

тржишту, продаје или изнајмљује у Републици Србији и која може да дескремблује дигиталне телевизијске сигнале, мора да има следеће карактеристике:

1) дескрембловање дигиталних телевизијских сигнала у складу са јединственим европским алгоритмом за скрембловање (Common Scrammbling Algorithm – CSA или Common IPTV Software-oriented Scrambling Algorithm - CISSA) којим управља ETSI..."

Образложење:

Предлажемо да се у члану 3. став 1. тачка 1) пропише да се за дескрембловање телевизијских сигнала које се врши у складу са јединственим европским алгоритмом за скрембловање, **поред алгоритма CSA користи и алгоритам CISSA.**

Наиме, заједнички алгоритам кодирања (или CSA - Common Scrammbling Algorithm) је алгоритам за шифровање који се користи у DVB дигиталном телевизијском емитовању за шифровање видео токова. CSA је прецизирао ETSI и усвојио DVB конзорцијум у мају 1994. године. Отварањем кода 2002. године CSA је постао јавно познат у целини, а криптоаналитичари су почели да траже слабости.

Када би CSA био разбијен, шифровани DVB преноси би били дешифровани, без обзира на то који се власнички систем користи за условни приступ. Ово би могло озбиљно да угрози плаћене дигиталне телевизијске услуге, јер је DVB стандардизован за дигиталну земаљску телевизију у Европи и шире, а користе га многи провајдери сателитске телевизије.

Због свега горе наведеног настала је потреба да се уведу нови алгоритми поред CSA, иако је то и даље алгоритам са доста великом поузданошћу.Једна алтернатива је CSA3, а друга CISSA алгоритам, чију употребу предлажемо за дескрембловање дигиталних телевизијских сигнала. Оба предложена алгоритма користе AES алгоритам као основу.

С поштовањем,

ГЕНЕРАЛНИ ДИРЕКТОР

Владимир Лучић