



DTA Security

Prepared for DSTAC WG3

Final Version

June 2, 2015

Topics

Overview of DTAs and DTA Security

DTA Security Platform Overview

TADA Security Platform Conceptual Overview

DTA Infrastructure

DTA Development Process

Overview of DTAs and DTA Security

DTAs – DTA Security – DTA Infrastructure

What is a DTA?

- Digital Transport Adapter – A low-cost, one-way device used to enable MSOs to economically upgrade subscribers to digital.
- Design constrained by regulatory prohibitions.
- Primarily used for the delivery of basic and expanded basic content on additional outlets.
- Viewer experience intended to match the typical analog TV experience.
- Does not support VOD or PPV/IPPV; QAM only solution.
- Variety of manufacturers.

What is DTA security?

- DTA security is a security system that is compatible and runs in parallel with ARRIS MediaCipher and Cisco PowerKey conditional access systems.
- Video streams are encrypted by the CA system and keys are delivered via ECMs to set-tops and DTAs.

What infrastructure changes are required to support DTAs?

- DTA Control Systems
- In-band EMM and data delivery
- Key co-ordination with existing CA systems

DTA Security Platform Summary (TADA Security)

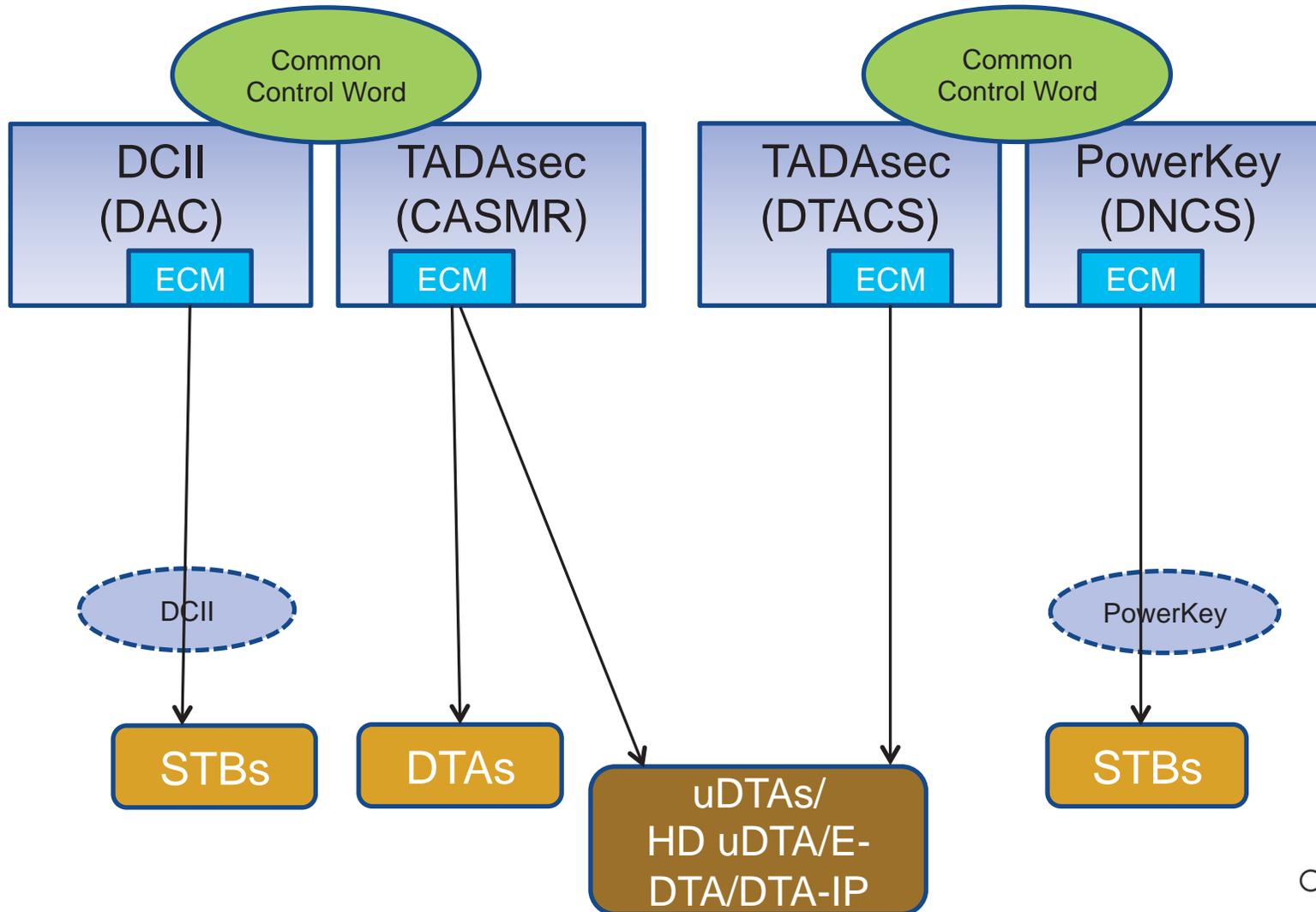
- **DTA Advanced Security (TADA)** is a security platform developed by ARRIS (Motorola), Cisco, Comcast, and CCAD and licensed by CAL.
- TADA is an anagram for “**DTA A**”dvanced Security.
- TADA is compatible with legacy MSO CA systems:
 - Conditional access for ARRIS (Motorola) systems
 - Conditional access for Cisco systems
 - “Universal” solution - Portable across ARRIS and Cisco systems
- A device using TADA can wake up on the network and discover which system it is in and use the correct CA technology for that system.
- TADA CA is based on SOC hardware security environment with a hardware root of trust (no CableCARD or separate secure ASIC required).

Device	Video Encryption	Key Ladder	Key Material
DTA	DES-CBC (SCTE-52)	ARRIS Proprietary	Provided by ARRIS
uDTA / HD uDTA / E-DTA / DTA-IP	DES-CBC (SCTE-52)	ARRIS Proprietary	Provided by ARRIS and Cisco
	DES-CTS	Cisco Proprietary	

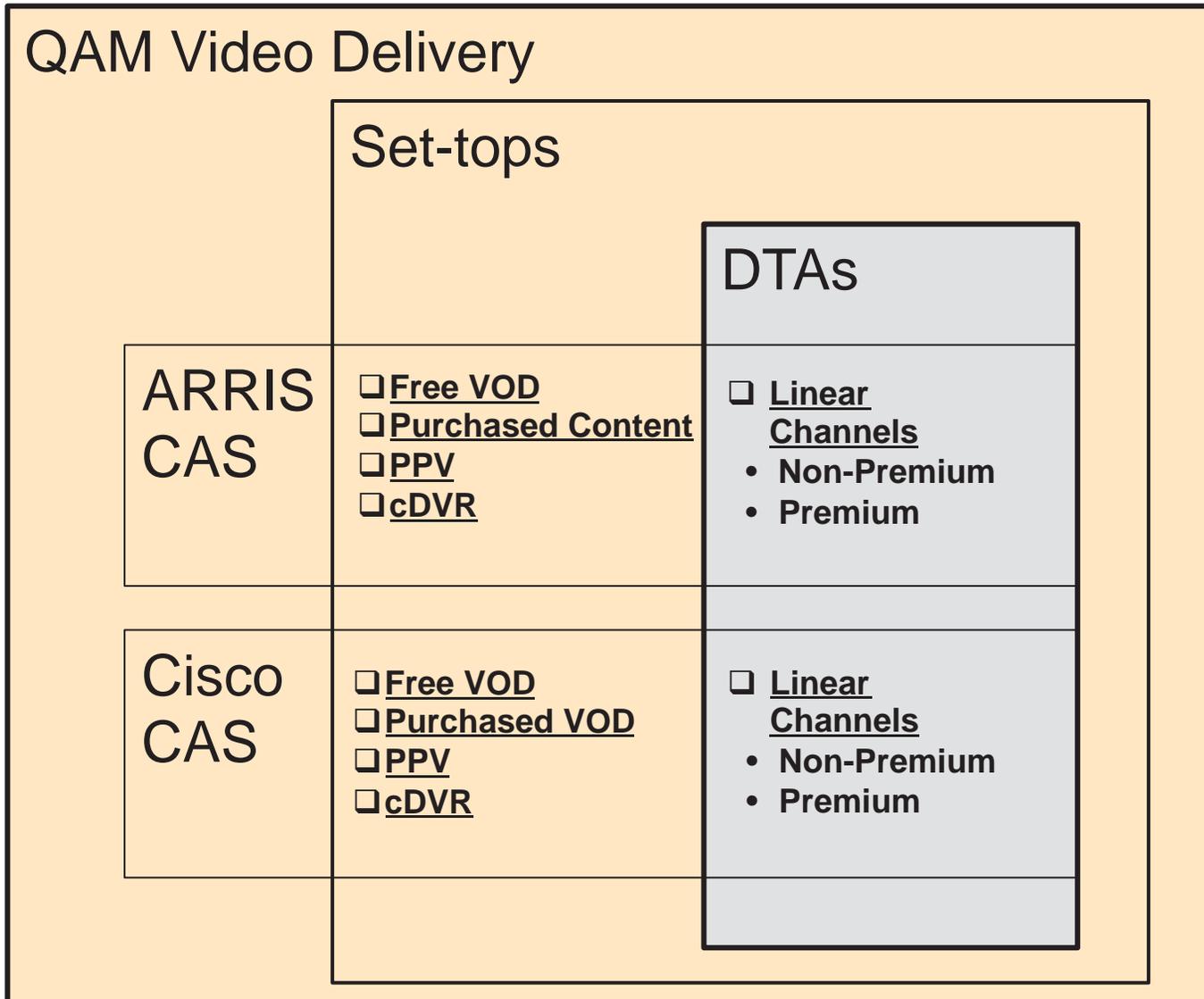
TADA Security Platform Conceptual Overview

ARRIS - CA Mode (SCTE-52)

Cisco - CA Mode (DES-CTS)

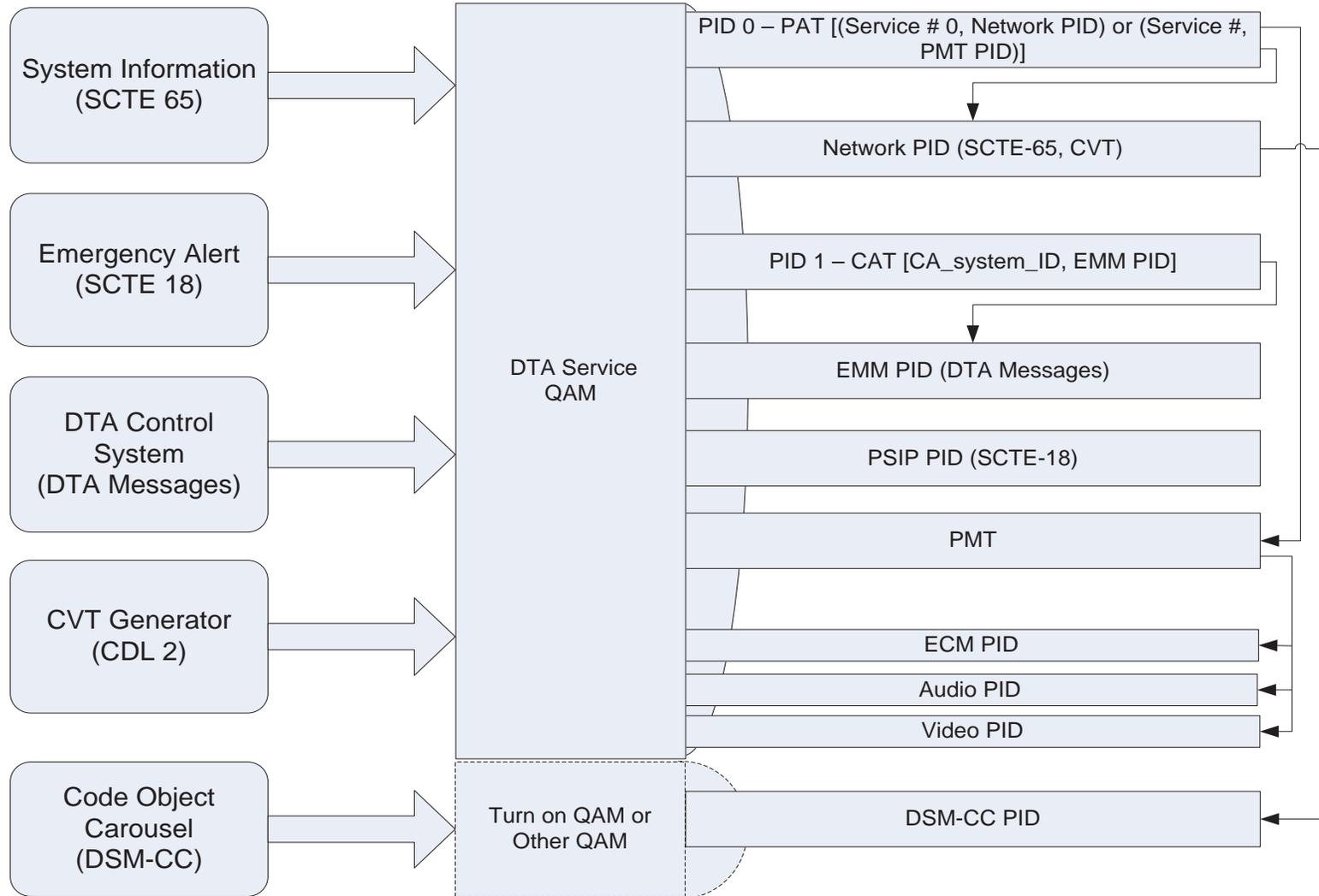


Video Services Accessible on DTAs - Comcast

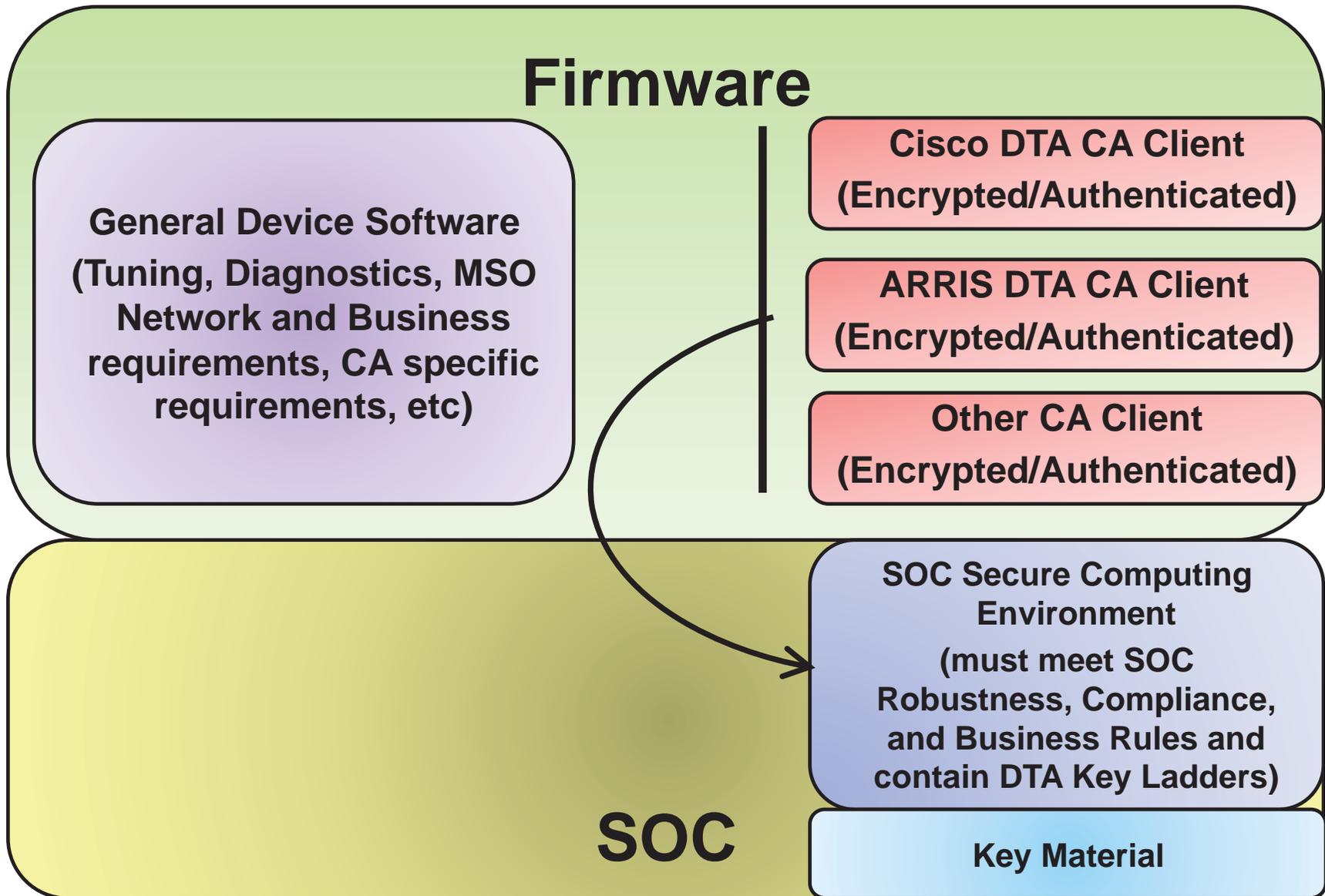


DTA/uDTA Infrastructure

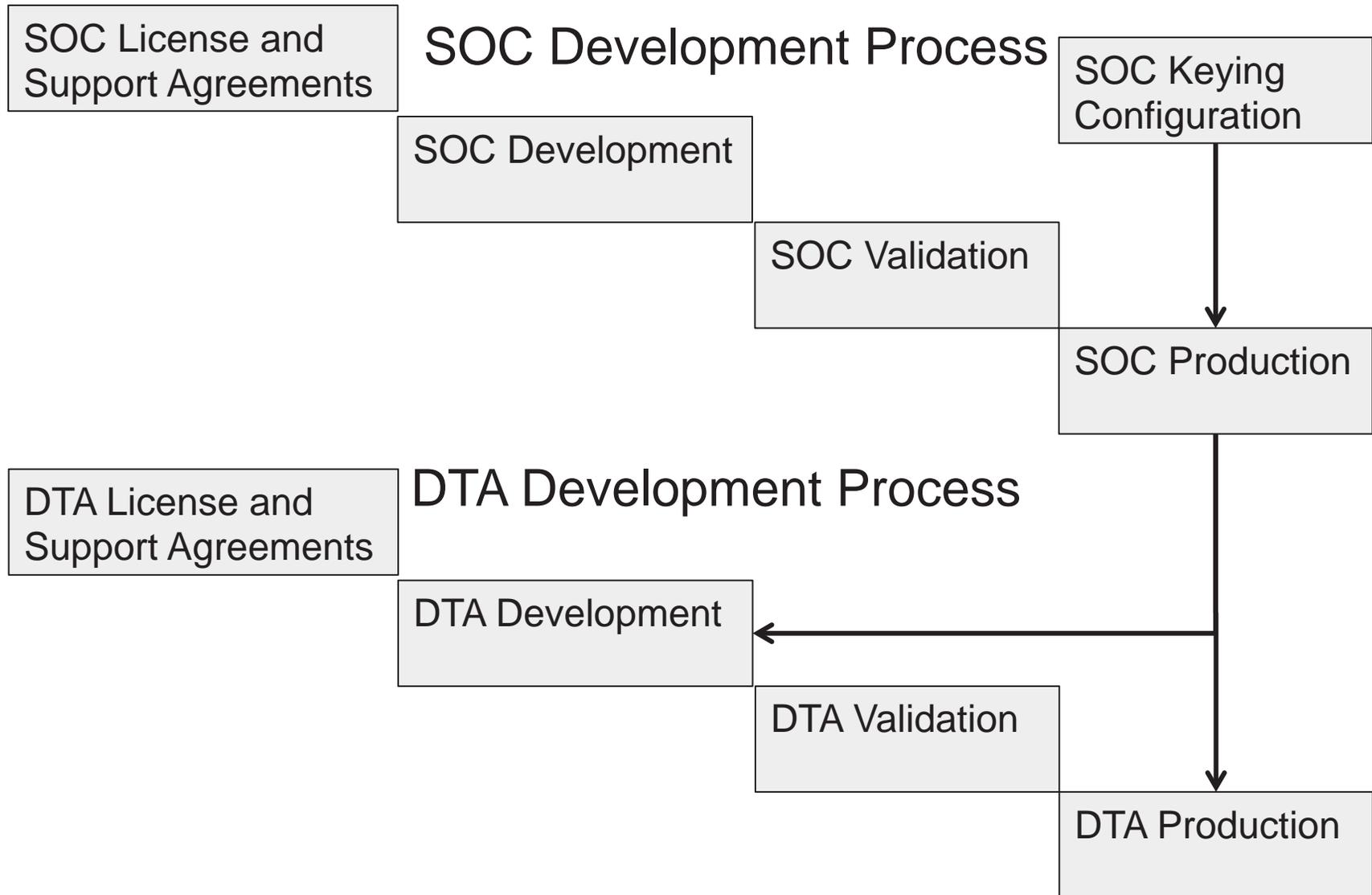
DTA In-band Data Delivery



HD uDTA Device Architecture – Conceptual Overview



DTA Development Overview



DTA Security Summary

- DTA CA Client is downloaded and executed in a secure processor in the SOC
- Custom Key Ladders are part of a DTA SOC
- Key Material is Provided by ARRIS and Cisco
- DTA Security is for linear QAM video services



Questions?



COMCAST