Historical Background

The current HbbTV specifications base their approach to trust on a long standing assumption in the TV broadcast industry, that the broadcast signal itself can be trusted. The theoretical possibility of an attack on the broadcast has been known for many years but there has been a broad consensus within the industry that an attack would be hard, expensive, illegal, higher risk for the attacker than web based attacks and unlikely to reach enough consumers to be worthwhile. The latter point was partly due to TV transmission characteristics and partly due to TV receiver implementations being very different from other devices.

As time has gone on, this assumption can be challenged for a number of reasons;

- TV receiver implementations are re-using more and more hardware and software from the tablet and smartphone industries. This makes it easier for an attacker to develop an attack for a TV than was the case previously when TV hardware was largely dedicated to the TV market and most software was developed from scratch by the manufacturer, their silicon supplier or a dedicated TV software supplier.
- The equipment needed to attack the broadcast signal has fallen in price and the tools needed for an attack are available as software for a PC rather than dedicated hardware.

Together these lead to a re-evaluation of the assumption that the broadcast can be trusted.

The security provisions in the current HbbTV specifications include the use of SSL certificates and the HTML5 Same Origin policy. However there are limitations with these provisions:

- Depending on the TV implementer, the consumer may not have visibility of when a secure link is in use.
- SSL/TLS provides a guarantee that a server name is what it purports to be but cannot vouch for the content served from it (which is also true for the web). Depending on the TV implementer the consumer may not have visibility of the server name and therefor the value of the guarantee is diminished.
- The delivery of the initial URL of the HbbTV application is only secure to the extent that the broadcast can be trusted (see above). Without a securely delivered application URL, the protection that Same Origin policy and SSL/TLS can provide is limited.