

XM Satellite Radio Grooves Over Secure Conditional Access

Security Builder toolkits and Professional Services helped ensure the success of XM Satellite Radio

"Certicom's strong encryption technology is a crucial element of our service as it protects the integrity of our content and ensures that only authenticated members have access to it."

– Derek de Bastos vice president of XM Satellite Radio

XM Satellite Radio Inc., headquartered in Washington, DC, is one of two FCC licensees to deliver subscription-based satellite radio programming. XM inaugurated its coast-to-coast, digital-quality service with 100 channels of music, news, talk, sports, comedy, and children's programming delivered via two geostationary satellites. The service is targeted to the nation's 200 million plus automobile and truck drivers as well as home radio users.

XM's state-of-the-art, all-digital broadcast center generates broadcast signals that are uplinked to two Boeing B-702 satellites from where signals are transmitted to subscribers. XM's business case relies on secure conditional access, to ensure that 100% of its listeners are paying customers.

THE CHALLENGE: the need for embedded security

Wireless communications environments present unique challenges with respect to controlling piracy and the resulting loss in revenues. The geographically diverse area to which content is delivered through these networks and the lack of a subscriber authentication feed back mechanisms further contributes to these challenges. Policing the authorized and unauthorized reception of these signals can be a formidable task.

XM recognized piracy as a significant risk to their business model and turned to Certicom to develop a robust Digital Rights Management (DRM) solution to mitigate this risk. DRM is the securing, controlling and tracking of digital content throughout its lifecycle. DRM and the protection of content are among the most complex problems facing the security industry today.

REQUIREMENTS

- **easy integration for accelerated time-to-market**
- **small footprint with minimal impact on performance**
- **scalability**
- **standards-compliant**
- **provides a strong support organization**

THE SOLUTION: Security Builder Crypto, Security Builder SSL and Professional Services

Certicom Professional Services was given the challenge of designing and building a DRM solution to mitigate the principle security threats of cloning receivers, eavesdropping, hacking and key theft. Certicom's solution incorporated embedded encryption, key management and security system management technologies to equip XM with a state-of-the-art broadcast encryption system that significantly reduced the risk of lost revenues due to signal theft.

Key components of the Certicom solution for XM included user-friendly activation and authorization, content protection, conditional access, renewability and manufacturability of the solution.

KEY BENEFITS

- **standards-based, interoperable, end-to-end security**
- **powered by Elliptic Curve Cryptography (ECC)**
- **rapid deployment for faster time-to-market**
- **increased security with minimal impact on performance**



THE RESULTS: embedded security

By selecting Certicom for its embedded security needs, XM Satellite Radio was able to successfully launch its offering confident that only authenticated members had access. XM Radio also enjoys the following benefits:

User-Friendly Activation and Authorization

User-friendly activation is a key feature of the solution; the goal is to avoid putting bona fide customers through a painstaking and time-consuming activation process. The heart of the solution is a unique hardware key that is burned into each radio during manufacturing and stored in a tamper-resistant memory location. This key is used to provide seamless activation and authorization.

Content Protection

Content protection is necessary in order to prevent piracy. Content is encrypted over-the-air so that only intended recipients can listen to and enjoy XM service. To protect against unauthorized replication or copying, the content is decrypted in tamper-resistant hardware, preventing attackers from obtaining a digital copy of the clear content.

Conditional Access

Conditional access is used to limit reception to legitimate subscribers. Conditional access relies on some secret information, some of which is burned-in the receiver, and other that is transmitted over the air on a Broadcast Authorization Channel (BAC). To block unauthorized users from access, only authorized subscribers receive keys to decrypt the content.

The XM solution also manages intellectual property and licensing rights. The managed rights system includes usage rules associated with the content (e.g., who may receive the content, geographical conditions, temporal conditions, parental control, etc.).

Renewability

Renewability enhances the long-term integrity of the solution through device revocation. If XM identifies that a radio has been cloning, XM can revoke service to that radio. This is essential to limit the cost associated with cloning. In addition, renewability is an essential component in the lifecycle management of digital content.

Manufacturability

Manufacturability of the solution is key to the success of the solution. Certicom worked directly with receiver manufacturers to ensure the proper design of security mechanisms and cost-effectiveness of the solution.

RESULTS

- **maximizes revenues by safeguarding against theft of service**
- **preserves the integrity of content by protecting against over the air content copying**
- **integrates security mechanisms transparently for an unimpeded user interface**
- **supports service renewability to manage the content lifecycle and enable revocation in the event of an attack**

About Certicom

Certicom is a leading provider of wireless security solutions, enabling developers, governments and enterprises to add strong security to their devices, networks and applications. Designed for constrained devices, Certicom's patented technologies are unsurpassed in delivering the strongest cryptography with the smallest impact on performance and usability.

About XM Satellite Radio

XM Satellite Radio Inc.'s founding was prompted by the radio industry's first major technological change since the popularization of FM radio in the 1970s: the creation of a third broadcast medium, transmitted by satellite. Today, XM transmits 101 discrete, nationwide radio channels to subscribers throughout the continental U.S. in digital sound from coast to coast.