

# IRDETO ACTIVECLOAK™ FOR ePUBLICATIONS

DYNAMICALLY SECURE eBOOKS, eMAGAZINES, PERIODICALS AND OTHER ePUBLICATIONS FOR DELIVERY OVER THE INTERNET TO POPULAR TABLETS, SMARTPHONES, PROPRIETARY eREADERS AND PCs WHILE PROTECTING MONETIZATION AND BUSINESS MODELS FOR CONTENT RIGHTS HOLDERS AND DISTRIBUTORS

The print-to-digital transition is well underway within the publishing industry today, with Amazon now selling more eBooks than print copies. Magazine, newspaper and other reading categories are not far behind, fuelled by the growing popularity of tablets, smartphones and various eReading devices. An inevitable consequence of this migration to digital consumption is rampant piracy which threatens the effective monetization of digital content and the long-term profitability of the industry. History has shown that every digital asset or device that is of economic or technical consequence has been hacked, without exception. Unfortunately, the static security methods currently used by the publishing industry are typically centered around DRM, and are a “one-time only” proposition that, once broken, remain broken.

What type of security solution is required to ensure that your application won't be hacked, your content pirated and your brand image tarnished?

A good security partner must:

- Provide a state-of-the-art security technology that does not impact the user experience
- Offer a sustainable, long-term security approach to protect your content over its entire economic life
- Apply it to all of the most popular reader devices, with a plan to supporting future devices as they come to market
- Be known and trusted to help you get the content you need

- Have a long-term strategy for maintaining the security of your application and your brand when it comes under attack
- Ensure your application gets to market as quickly as possible
- with all necessary approvals

These are all the hallmarks of Irdeto ActiveCloak for ePublications.

## IRDETO ACTIVECLOAK HIGHLIGHTS

Irdeto ActiveCloak for ePublications is a comprehensive solution to secure eBooks, eZines and other digital publishing content on any consumer device. Irdeto provides:

- Solutions to secure content on the latest devices supporting iOS, Android, Windows, Mac and proprietary readers
- Invaluable experience in protecting high-value digital content for more than 300 licensees and distributors worldwide, including consumer entertainment brands Comcast and Netflix
- Core technology deployed on more than 2 billion devices and applications over 10 years
- Nearly 100 years of publishing industry heritage as a wholly-owned subsidiary of the Internet and media conglomerate Naspers

## REDUCE YOUR RISKS WITH A KNOWN AND TRUSTED SECURITY SOLUTION

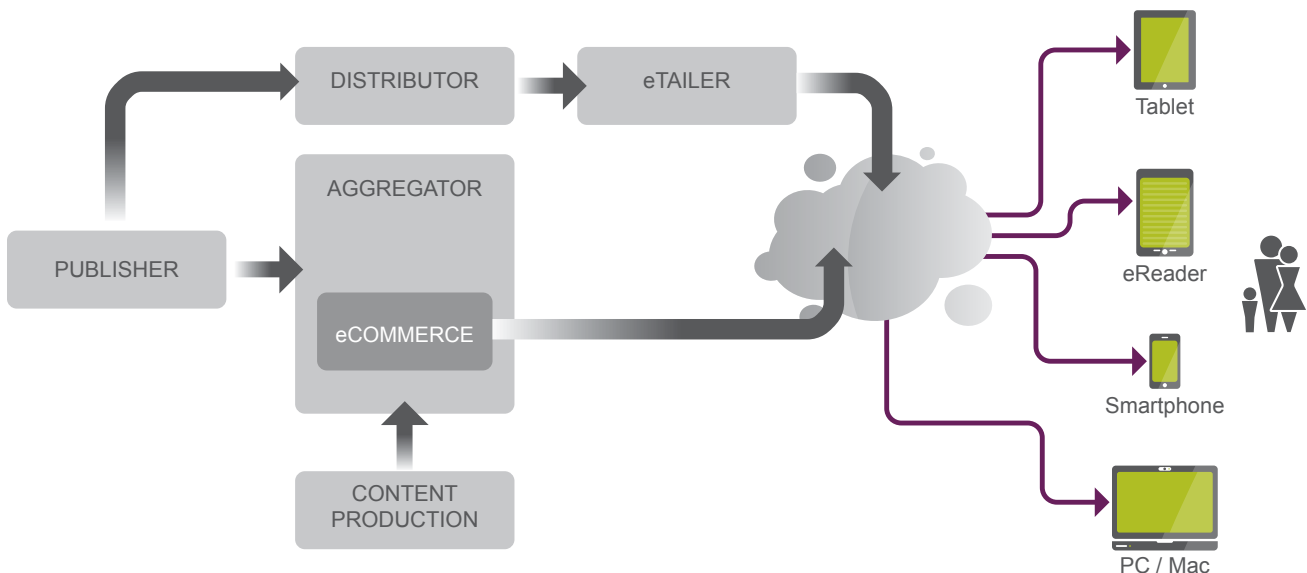
Creating an application for any platform that will stand up to the threat of piracy is no trivial matter, and many off-the-shelf security solutions may not meet your needs; especially your long-term ones. According to Jeannie Mullen, CMO at Zinio, a leader in the delivery of digital publications and the world's largest and most popular global magazine newsstand that has partnered with Irdeto to develop an effective security solution for eZines:

*"The digital piracy problem we all face will not fix itself and will only get worse until we find a comprehensive security solution that is both renewable and software-based to grow with our business."*

Being able to launch new products quickly with a minimum of risk is critical given the quickly changing marketplace. The eReader-enabled devices consumers love to buy and use are increasingly open and difficult to secure. Content provider security requirements are also in flux as new technologies constantly come to market. While tablets, smartphones, and dedicated eReaders all have tremendous consumer interest, they also have significant security threats associated with them. As a result, security solutions must be proven and battle-tested, trusted by rights holders and provide a range of options for integration with any device. Only by doing this can you securely expand your brand and increase your subscriber base, regardless of how the world around you changes.

| Category     | Feature                 | Key Benefit  |
|--------------|-------------------------|--|
| Publishing   | Watermarking            | Insert unique content identifiers to trace source of the content   |
|              | Content Tracking        | Scan and report on where content is being leaked from by monitoring peer to peer and other online redistribution sites |
| Distribution | Platform Security       | Ensure proprietary online delivery platform is tamper resistant  |
|              | DRM Security            | Ensure the DRM is robust and hardened using layered security to prevent tampering                                      |
|              | Diversity               | Deploy diverse application instances to reduce impact of attacks   |
|              | Renewability            | Update security on deployed applications to combat evolving threats  |
| Consumption  | Application Security    | Protect reader apps on Android and iOS devices and PCs/Macs to help prevent content theft                              |
|              | eReader Device Security | Harden software on proprietary reader devices to protect against tampering   |
|              | PDF File Security       | Prevent copying, screen scrapping, redistribution of eBook and eZine PDF files.  |
|              | HTML5 Security          | Future-proof protection for HTML5-based content to prevent copying and screen scrapping                                |

## ePUBLICATIONS DELIVERY OPPORTUNITY



## IRDETO ACTIVECLOAK™ FOR ePUBLICATIONS

Irdeto is the only company with the content security expertise and delivery track record to enable electronic publishers and distributors to license and securely deliver content to any device their readers own.

Irdeto ActiveCloak already protects digital content for the world's leading media providers; extending this technology to digital publishing is the next local application of this technology.

ActiveCloak for ePublications provides end-to-end security and business model value:

### End-to-End Security

- Protect Digital Assets
  - Crypto Keys, Content, Software
  - Protected even in use
- Protect Content Rendering
  - PDF, images (JPEG, PNG)
  - HTML5, EPUB3, video, audio
- Protect Content Lifecycle
  - Content reporting and tracking
  - Monitor hacker activity
  - Develop Countermeasures
  - Deploy renewed security

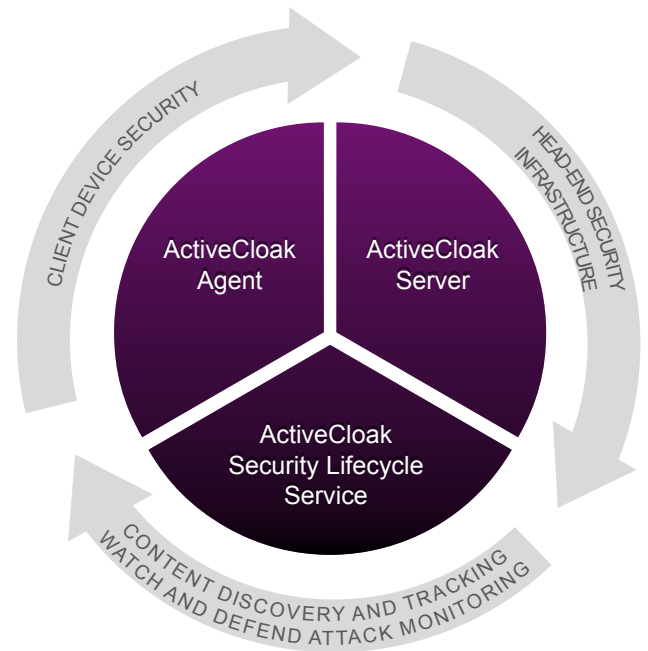
### Business Value

- Protect Business Models
  - Protect monetization by controlling media
  - Multi-platform solution covers the entire addressable market
  - Disrupts pirate business model
- Protect User Experience
  - ActiveCloak protection is invisible to the user
  - Flexibly balance security level and performance

## THE SOLUTION

Irdeto ActiveCloak combines server-based software, client-device software agents and services to create an effective lifecycle security approach to protecting digital assets. The server-based modules provide the necessary infrastructure to create the security-hardened client agents which reside in reader devices.

## ActiveCloak Lifecycle Security



### ACTIVECLOAK AGENT

The ActiveCloak Agent implements client device functionality and security for the reader application. Its main functions are to:

- Secure digital assets, such as keys, certificates, and data
- Continuously monitor the application's integrity and that of the surrounding components it interacts with (anti-tampering)
- Ensure that assets are bound to the unique device where the agent is running (anti-cloning)
- Provide a secure framework SDK for integration into the reader application

The ActiveCloak Agent is protected using Cloakware core technology such as White-Box cryptography, source code transcoding and binary tools. It is available for deployment on multiple device platforms.

- Integration with a single, simple application programming interface (API)
- Robust client content protection for license acquisition, rights management, and if the license permits, decryption of manifest and content files as appropriate.
- Client-side Individualization to node-lock the content to the device
- Core security allows only authorized applications to access runtime functionality
- Prevent tampering or unauthorized access to the rendering path
- Verify platform, eReader and operator UI
- Detect hacked and rooted devices

## ACTIVECLOAK AGENT GENERATION MODULE

Diversity is an important way to make piracy economically unattractive, because it forces the pirates to divide their attention among many different code sets, with limited reward for breaking any individual code instance. This module produces diverse ActiveCloak Agents to meet your ongoing, enhanced security needs.

The Agent Generation Module is an off-line utility which provides the following functionalities:

- It creates diverse instances of the ActiveCloak Agent, each with a unique random seed
- It customizes the Agent's features and capabilities by using a configuration file established for your environment (functions, platform and security profile)

## ACTIVECLOAK RESOURCE PROTECTION MODULE

This module secures the cryptographic assets (keys, certificates, etc) and packages them by using patented Cloakware White-box cryptography and signing technologies. Assets can now only be used by the ActiveCloak Agent on the device.

The Resource Protection Module is an off-line utility providing the following functionalities:

- Enables the secure deployment of assets and data, such as DRM keys and certificates, to a device
- Protects assets and data in a secure store by using White-Box cryptography and data transformations
- Signs applications to enforce access control at runtime

## ACTIVECLOAK INDIVIDUALIZATION MODULE

This module binds (node-locks) secured assets to an ActiveCloak Agent within a device, so that assets can only be used on the target device. This is implemented in the client device and executed at first run, thereby binding the assets to the device fingerprint.

- Enables node-locking, which binds a secure store to a specific device or platform, so that it can only be used on that target device or platform (anti-cloning protection)
- Defines the access mode for a secure store (read/write or read only)

## SECURITY LIFECYCLE SERVICES

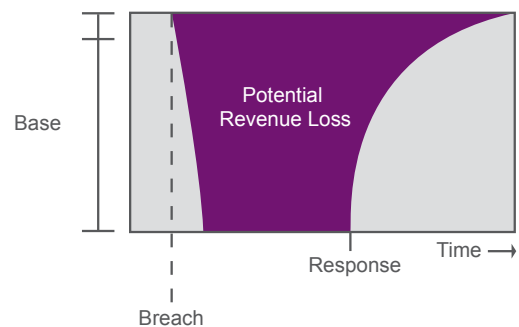
The typical approach to application or device security is to assume that the initial design will remain secure over time. However, the reality is that, given enough time and effort, any security system can be compromised. For this reason, the Irdeto ActiveCloak solution is designed not only to provide the very highest level of initial attack resistance available in the industry, but also methods to anticipate and mitigate attacks that occur over time. ActiveCloak Security Lifecycle Services provides an effective mechanism to react in the event of a breach, and

includes unique elements to limit potential damages and enable quick deployment of countermeasures in order to ensure the ongoing integrity of the system and protection of content.

## TRADITIONAL SECURITY MODEL

In a traditional security model (without built-in security lifecycle measures), the lack of a recovery strategy leads to:

- Longer term piracy or loss of platform integrity
- Withdrawal of content provider licenses
- Platform obsolescence
- Impacts on the consumer and damage to your brand

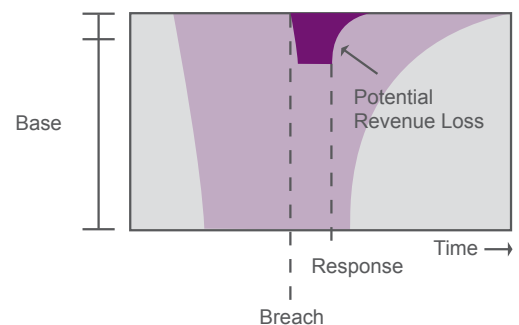


The loss of revenue over a sustained period is appreciable, and sometimes breaches are not even recoverable.

## IRDETO DYNAMIC SECURITY MODEL

In the Irdeto model, the impact of a security breach is mitigated because:

- Diverse instances of the deployed application code mean that a hack on a single version does not affect other versions
- Recovery can be rapidly achieved through ongoing monitoring and being prepared to respond BEFORE significant harm is done
- Countermeasures can be rapidly developed and deployed to disrupt potential hacks and rectify security breaches



This approach leads to a minimal disruption of your business in the event of a security attack.

Irdeto's Security Lifecycle Services provides a suite of services to ensure that the barrier for a security compromise is always maintained as high as possible at any given moment. These services protect your digital assets and associated business model over the full lifecycle of the product and the underlying platform.