DATA™ 443 | ARALOC™ CORPORATE SOLUTIONS

# Enterprise Content Protection and Distribution

Security and Protection Frequently Asked Questions

DATA™ 443

ARALOC is an end-to-end DRM and content management system that offers corporate clients and content providers a flexible platform for the secure distribution, content management, viewer tracking and reporting analytics of any digital media content.

# Table of Contents

*The information contained in this document represents the current view of Data443™ Risk Mitigation, Inc. on the topics discussed as of the date of publication. This implementation guide is for informational purposes only. Data443™ Risk Mitigation, Inc. MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. This information is subject to change without notice.*

*Data443™ Risk Mitigation, Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Data443™ Risk Mitigation, Inc., the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

## General Security

### What type of encryption does ARALOC use?

ARALOC uses 256 bit AES encryption using a symmetric key system.  In a symmetric key system, there is no public key, but rather a single private key that is only released to authenticated users. Each piece of content is encrypted with a unique key. With a 256-bit key, the possibility of an unauthorized user guessing the correct key is 1 in 1077. Scientists predict that it will be nearly 200 years before we are capable of building a computer that has the power to attempt to break this type of encryption.

### How does ARALOC store and manage content cryptographic keys?

ARALOC utilizes a proprietary key management system designed to secure keys while providing convenient access to end users. Encrypted ARALOC content contains metadata that instructs ARALOC secure apps to contact the ARALOC Management Console to obtain a key. If the user successfully authenticates and has rights to view the content, the system downloads the encrypted key and decrypts the content for the duration of the user's view.

### Are encryption keys stored on the end user's PC or device?

ARALOC allows the content owner to select whether or not a key is stored on a user's PC or device. If an encrypted key is stored locally, this allows the end user to view content while offline.

### Where are the content usage rights stored?

Usage rights are stored within the encrypted content package, and on the server. If offline access is allowed, the ARALOC app will use the most recent version of the content usage rights. If the user is online, and/or if an internet connection is required, the content usage rights on the Management Console will be considered the most recent.

### Where are the user credentials stored?

By default, ARALOC's user credentials are stored in the cloud alongside the Management Console. ARALOC supports integration with LDAP and other identity systems to authenticate your users. Please speak with your Data443 representative for more details on our integration services.

### Does the ARALOC System support token authentication systems such as RSA SecurID?

Token authentication systems are implemented by organizations to authenticate users who are attempting to access secure systems or log on to a virtual private network (VPN).

In a typical ARALOC implementation scenario, the token would be utilized to allow the mobile device or computer to access an internal network via a VPN. ARALOC would then use the authenticated, secured channel to download encrypted ARALOC content to the mobile application or desktop.

Custom security integration options are available for organizations that require use of tokenbased authentication within ARALOC itself. Please speak with your Data443 representative for more details.

## ARALOC **Environment**

### Where is the ARALOC Management Console and database located?

ARALOC and its supporting databases and servers are managed by and hosted in the Microsoft Azure Cloud. (CaaS)

### How is physical security managed at the Microsoft Azure Data Center?

All Microsoft Azure “Data Centers” maintain state-of-the art physical security, including floor to ceiling concrete construction, steel doorways, 24x7x365 surveillance, environmental protections and extensive secure access policies. Please ask your Data443 representative for additional details. How is network security managed?

The ARALOC server sits behind a secure network that includes hardware and software for threat monitoring, hardened router configurations that provide traffic monitoring and protection from port scanning. Please ask your Data443 representative for additional details.

### How is my organization’s and user’s private information kept secure?

Local passwords are protected using a one-way hash. ARALOC provides extensive logging and auditing capabilities that can monitor system interactions at the database, administrative and user level.

### How is my organization’s information separated from other clients?

Data, users, content and encryption keys are tied to a specific client. ARALOC does not allow the sharing of data between clients. Private cloud hosting of a client-specific ARALOC installations is available. Please contact your Data443 representative for more details.

## ARALOC Apps

### What is an ARALOC App?

An ARALOC App is an application used to enable the purchase or distribution of content, authenticate users, obtain keys, and display content. Apps are currently available for iOS, Android and PC/Mac. ARALOC can protect a single piece of content and display it on multiple devices.

### How do the ARALOC Apps protect my content?

The ARALOC Apps will not download a decryption key or display content without first validating the user credentials. Afterwards, the ARALOC App will enforce the access rights defined for the client or content.

While viewing, the ARALOC App protects your content in various ways. Cutting and pasting is restricted, and screen capturing tools and utilities are blocked. This prevents a user from easily making a copy of protected content.

### Can any encryption software protect my content from users who use a camera to take a picture of their monitor?

No encryption or protection software can prevent an authenticated, valid user from the premeditated use of a camera, external audio recorder, or video camera to copy content.

### Can my organization obtain a customized version of a mobile ARALOC App?

Yes.  The ARALOC App is designed to be branded and distributed via all supported channels, including App Stores and direct distribution. The ARALOC team can customize and configure an ARALOC-based application in a fraction of the time typically required for a new mobile application

## Content and Supported Formats

### What types of media does the ARALOC DRM system support?

ARALOC supports a variety of formats including audio, video, PDFs, HTML 5 interactive, web content, and MS Office documents. The ARALOC publisher can intelligently identify the type of content, convert it as appropriate, and protect it.  For example, iOS devices can display Microsoft Word documents natively, while Android devices cannot.  In this case, ARALOC would convert the Word document to HTML and store it alongside the native Word document. The App for the device will decide which format it can use.

### Does ARALOC support HTML5 and Flash Video?

HTML5 and other rich media are supported up to the limitations of the device.  In general, if the device can display the content in its native browser, ARALOC will be able to protect it.

For example, while ARALOC can protect Flash video, Apple does not support Flash content on iOS devices, so that content will be unable to be displayed in an iOS device.  In that case, converting the video to mpeg4 would allow the video to be displayed on all devices.  Your Data443 representative can answer any questions regarding specific content support.

## ARALOC Publisher

### What is the ARALOC Publisher?

The ARALOC Publisher is a Windows-based software product used to encrypt ARALOC content and set the initial access rights. The publisher can also automatically transmit protected content to a storage location for later distribution to mobile devices.

### How does the ARALOC Publisher manage encryption keys?

When a new piece of content is ready for encryption, the publisher requests a new key from the ARALOC Management Console. A new key is generated and transmitted to the publisher.  The key is not stored on the file system, and is not available after the encryption is complete.

### How is access to the ARALOC Publisher maintained?

The ARALOC publisher is available via the ARALOC Management Console. Only authenticated “publisher” users can access the console and launch the publisher.

### How does the ARALOC Publisher transmit encrypted content?

Encrypted content is transmitted over encrypted SSL to a configured WebDav server. (optional) Data443 can provide content hosting services, or content can be uploaded to a customerowned WebDav server.

## ARALOC Software Security

### Has a security assessment been performed on the ARALOC Management Console and Database?

Yes. A comprehensive security assessment was conducted by independent consultants. These consultants were/are employed with firms such as RSA, Mandiant, Booz Allen Hamilton, and Verizon Business. These consultants hold numerous security certifications including, but not limited to, GIAC Penetration Tester (GPEN), Security+, Certified Ethical Hacker(CEH), and GIAC Web Application Penetration Tester (GWAPT).

### What was the scope of the security assessment?

The consultants conducted:

- Configuration reviews of hosting servers
- Configuration reviews of network appliances
- Vulnerability scans of Hosting Server OS
- Web Interface tests.
- Checks for OWASP top 10 issues and others, including Code Injection, Privilege escalation, and horizontal account movement.
- Tests of ARALOC Apps - traffic capture, code review, decompile and process analysis.

### What was the result of the security assessment?

The assessment discovered three issues that were remediated as described below.

- Host OS Vulnerability - Remediated due to move to managed servers located in the Microsoft Azure Cloud.
- A limited number of user input points on the Management Console were identified as vulnerable to injection. Remediated.
- ARALOC Java Based App - possible content exposure between decrypting and viewing process. Remediated.

### What methodologies does Data443 use to ensure the security of its mobile applications?

ARALOC manages users, content, security keys and permissions on the ARALOC Management console. Without first knowing a user's name and password, it is impossible to download a key and decrypt protected content. All communication between the server and the client are encrypted, and cannot be read via a proxy.

On mobile devices, we provide several features to provide the highest levels of security:

- The ability to never store keys locally, always requiring internet authentication.
- All user information is encrypted locally using ARALOC technology.
- Not utilizing or clearing caches as needed.