RDocs™

Whitepaper
Document Security

Track Readers. Kill Documents.
Control Content Even After Sent.

RPostDocs.io

Contents

RDocs™ by RPost®

This whitepaper examines RPost's revolutionary approach to Digital Rights Management for documents that honors its lifelong commitment to feature-rich, affordable security-centric software services that are intuitive and easy to use for all parties involved.

RPost thrives on being artisans and experts in everything they do: secure and certified email encryption for privacy and compliance; e-signatures and web forms to ease digitization of workflows; e-delivery tracking to prove important communications; managed file transfer to simplify secure sharing of large documents and sets of files; document-level digital rights management to empower control of document access even after transmission; and AI-infused apps to prevent data leaks by minimizing human e-security errors.

This RPost document security product, RDocs™, is a natural continuum of its mission: to help its customers worldwide communicate and transact electronically in the most secure, compliant, and productive ways possible and to continuously innovate its products to support their evolving needs.

This is why more than 25 million users have enjoyed RPost software services for two decades in 193 countries. Those software services, in addition to RDocs, include RMail® email security, Registered™ e-compliance, RSign® electronic signatures, and RForms™ click-build e-forms.

The Digital Rights Management Landscape

There is a category of **information rights management** or **digital rights management** software applications that are designed to add power to track and manage access to files after they have been transmitted onward, such that they can be entirely controlled, revoked, unsent, or expired by the file originator.

This technology has become ubiquitous within the online entertainment industry to protect copyrights related to music and video file intellectual property. This technology enables, for example, consumer-centric online video "renting" where the video may be streamed or downloaded by an end user and expired after a set period of time. Important to note: these videos or music files require compatible software by the viewer to play – and thus for the copyright enforcer to be able to revoke or expire access.

As enterprise technology has been incorporating trends from the consumer landscape, and especially with the outburst of the Covid-19 pandemic accelerating remote work everywhere, the business world has witnessed an unparalleled demand to distribute documents outside of the corporate firewall (to home offices, for example). And so, the ability to share digital files securely, protect sensitive information even after the share and control who can access what, where, and when, has become a general necessity.

Further, with the changed work environment, there has been a demand for more work with limited human resources. This has increased the risk of human e-security errors that often lead to sensitive information being accidentally distributed to the wrong recipients. In addition, sophisticated social engineered cyberattacks like impostor lures and Business Email Compromise are now more widespread than ever. Thus, today there is a greater need to control access to a document after the send – to "unsend" -- in case a sensitive attachment to an email is misaddressed (accidentally or through a cyberthief lure).

With relation to "unsending" documents, the recently released functionality by Apple that allows users to, precisely, "unsend" messages is of utmost relevancy in this market. Although Apple did not invent the functionality (avant-garde consumer apps like Telegram released it years ago, and were followed by Meta's Whatsapp, Facebook Messenger and Instagram Messanger), it is no secret that Apple's go-to-market strategy often relies on releasing functionalities only after they have been thoroughly tested by other companies, and once there is high demand for them in the mass audience, as opposed to only tech-savvy early adopters. With this in mind, the fact that the "unsend" functionality has now been released for iPhone users is very telling about the **maturity of the mass consumer's concern about the future life of the content generated by them**. Technology-wise, text messages are traditionally stored in centralized servers, and as such, it could be argued the capability to "unsend" has been there all along, although only recently it has been made available at the UI level for end-users. Differently, in Digital Rights Management world, storing content in a centralized location is hardly recommendable as it would pose severe risks for compliance with GDPR and other data privacy laws and regulations. In this respect, RDocs technology is truly groundbraking as it allows to revoke access to a document that has already been downloaded and stored in the recipient's local device.

Lastly, tracking popularity of a music of video shares/streams after distribution, or tracking and cataloging who is viewing what when, empowers content originators or distributors with insights that they can use to further market, re-target viewers, or otherwise monetize. This same power can be provided to document originators through the use of digital rights management technologies for documents. Following iPhone's release of consumer data protection features ("Ask App Not to Track"), the ability for companies to gain insight into their consumers' online behavior has been severely affected. Meta alone is expected to lose ten billion US Dollars, and similar figures are reported for Alphabet, Snap and Twitter. This new scenario adds another layer of relevancy for services like RDocs that allow to capture consumer interest for marketing efforts.

Traditional Approaches to Enterprise Digital Rights Management for Documents

There are three traditional types of information rights management or digital rights management software employed in the market for documents, and now a new unique fourth. The three traditional systems have been commercialized within categories that we refer to as (1) Same Licensing Plan, (2) Install App, and (3) Centralized Storage.

1. Same Licensing Plan

"Same Licensing Plan" refers to those digital rights management software applications where viewers need to use not only the same software as the file originator, but also have the proper licensed access to the software in order to view the rights protected document. An example of digital rights management software that requires the intended viewer to have the same software and the proper licensed access level is Microsoft's Azure Information Rights Management software.

A major shortcoming of these systems is that they impose software installations and often premium licensing costs on the viewer. As such, all originators and viewers need to be in a software environment where there is a central IT organization managing software licensing with the proper license structures per user. While this may be practical for some companies, for many it is not. Further, when communicating documents to external parties outside of the corporate network, the originator has the added complexity of not knowing which of their recipients might have the proper software and licensing plan to access.

Determining which viewers have what software versions and who should be billed for the cost of upgrading to the proper licensing plans for access to view is a scenario that is even more untenable if opting to transmit to external parties out of the control of the originator's organization.

2. Install App

"Install App" refers to solutions that require viewers to install a proprietary app – also called "companion software" -- to access shared documents.

A major shortcoming of "Install App" companion software systems is that viewers must learn how to use obscure third-party software to access the files. This scenario is even more untenable if the intended viewer is in an organization that restricts unvetted downloads of software to company devices, which is often the case in professionally managed IT organizations.

3. Centralized Storage

"Centralized Storage" refers to applications intended to store documents in a shared, access-controlled repository; with those documents viewable in that repository after a designated viewer creates an account and logs in.

A major shortcoming of these systems is that they require viewers to create an account, which may cost the file originator extra platform access "per user" fees. In addition, "Centralized Storage" applications often do not provide protection against unwanted downloads or do not provide visibility as to what happens to the documents if downloaded or after further transmitted, and there is no mechanism to track sharers of screen captures or printed versions.

Furthermore, with these systems, the Originator may need to ensure that the particular rights-controlled files are in a separate isolated storage directory from other documents to ensure the intended viewers do not have access to view unintended documents - a scenario that is even more untenable if the intended viewer is viewing documents from multiple different senders or associated with multiple different projects and/or the Originator is managing multiple types of documents intended for a variety of viewer types.

These systems also challenge senders to keep track of who has access to what folder and with which documents, where an error can cause the Originator to fall out of compliance or fact of storage of the documents may be forgotten (left online) and cause future potential embarrassment or ongoing storage costs.

The New Fourth: Ubiquitous Access.

The fourth approach – a new age for digital rights management for documents -- we call "Ubiquitous Access". RDocs by RPost offers the only "Ubiquitous Access" digital rights management system for documents in the market. It's patented and patent pending[1] technology solves challenges of the traditional approaches by allowing organizations to share documents securely, controlling every aspect of the who, what and where even after the share. RDocs technology (1) does not require any software or special licensing for the viewer, (2) does not require any special companion software for the recipient, and (3) is a decentralized model – providing for all of the controls of, for example a "data room" but with no need to have centralized storage (which is a significant advantage for compliance with data privacy regulations).

RDocs is able to do all of this and more, thanks to its home grown, patent pending **Rights Protected Document**™ files, also referred to as an **RPD**™ files.

The Dusk of PDF – Portable Document Format file

For years, businesspeople converted documents into PDF files, mainly with the intention to signal that the document was in final form, not intended to be editable, with its formatting and content integrity preserved. For many, PDF file meant un-editable, protected, and formal.

With today's ubiquity of PDF editing and other software tools, PDF files have lost the public's notion that it is a protected un-editable format.

In addition, PDF files historically afforded many advanced controls that could be programmed into the PDF file with Javascript, but which require the viewer to use PDF "reader" software – special companion software for the reader/viewer. In recent years, PDF "viewer" technology has become ubiquitously built into web browsers, and as such, a generation of computer users stopped installing PDF "reader" special companion software. As a result, today there is low level of adoption of PDF "reader" companion software, a trend that is expected to continue in the coming years. As such, senders can no longer count on people that receive PDF files to have the right companion software to make the advanced PDF programmable behaviors function. Not knowing if the viewer has the proper experience makes reliance on these unworkable when communicating to external parties.

Most of what has been traditionally distributed as PDF files – whether manually or with output management or document builder tools - would be better served to be sent as RPD files. Why? Simply put, RPD files visually look the same to a viewer as PDF files opened in a web browser, yet RPD files build in the protections that many believe are native to PDF files but are not really available to PDF files.

While PDF files allow for some level of protection, such as limiting copying, printing or requiring a password to access (all of which are often defeated with no traceability as to, if defeated), once shared, the document is out of the control of the originator. This poses severe limitations for PDF files in the case that a document is accidentally misaddressed, misdirected, distributed without authorization, or if the originator would simply like to end availability.

The Dawn of RPD™ – Rights Protected Document file

RDocs overcomes the above-mentioned challenges by use of its inventive RPD™ file construct where security and controls that the file originator prescribes are built into and are self-contained inside the

[1] Patents listed at rpost.com/patents and US patent application number #63/363,014

RPD file itself; which displays to readers as an .HTML file, and can be saved and stored just like any file, and opened in any browser or .HTML file viewer.

There are a number of benefits to RPD files for both document originator and viewer:

- Viewers can access the shared content without downloading or installing special companion software or plug-ins, and without creating an account or incurring added licensing costs.
- Originators can at any time revoke access temporarily or permanently, kill a document entirely even after delivery, including all traces of the transaction.
- Documents are delivered directly to each recipient – there is no storage of documents by a third-party, which reduces compliance and data loss risks.
- Originators receive real-time insights as to who is viewing what document, when and where; with optional tallies of reader sentiment or feedback related to the content. These are document-level insights (vs. email delivery and opening or link click insights).
- Originators may choose to protect the content in the document with document-level security, which persists while inside the recipient's email inbox, and persists regardless of whether an email or file transmission is secure.

Further, there is an entire industry of Enterprise Output Management (EOM) software that deals with the organization, formatting, management and distribution of data that is created by enterprise applications like banking information systems, insurance information systems, ERP (enterprise resource planning systems), CRM (customer relationship management), document builders, PDF-generation, document scanning, document electronic faxing, retail systems and many others.

These systems construct a file from inputs and often prepare that file as a document compiled in PDF format for storage in a web system, transmission by API or transmission by email.

In the early days of output management systems, these files would become images of a document in a TIFF format which is a static format. Then PDF files became the standard, which includes the ability to apply some basic static controls to the document (like password protecting).

RDocs, with its RPD file, provides a new output file type option for output management software. This marks the dawn of a new era -- of powerful security, access control, viewer insights, and document-level interactivity that is tied to output management systems.

The enterprise output management systems, as they are compiling the document from various data sources, can generate the output file as an RPD file type (vs. a PDF file type) with the controls information required for that file as prescribed by the situation. The result is a generated RPD file returned into the output management system and dropped into whatever file repository or transmission process normally occurs for storage and/or transmission to a recipient.

Since any document, presentation or PDF can be converted into an RPD file with a few clicks or automatically, and to a viewer the user experience is the same as viewing a PDF, one would be hard pressed to think of a situation where there would be effort to convert a high value document into a PDF file and not want to have the tracking, visibility, access and other controls, or interactivity afforded by an RPD file.

RDocs Service Acts as the Conversion Engine to Generate RPD Files

The RDocs service empowers users to convert any document or presentation file (e.g., .DOC, .PPT, .PDF) into an RPD file. It additionally permits the document originator to tailor the controls associated with the RPD file.

From a user perspective, there are two roles:file originator and file viewer. Controls are set up by the file originator and are imposed on the file viewer.

The originator can use a web user interface to set their default controls or may set controls on a per message basis. The originator may opt to (a) send the file attached to a message with the indication of which controls to apply to the file, and have the file uploaded or attached to an email message, and transformed into an RPD file en route to the recipient (viewer); or (b) submit the file to be converted with the indication of which controls to apply to the file, and have the file returned (downloaded) to the originator transformed into an RPD file for later sharing. These two user experiences may be built into apps, output management systems, or web user experiences using API connections to the RDocs servers.

The controls that the originator may apply to the file are broadly grouped as follows:

Access Controls

RDocs converts any presentation or document into a Rights Protected Document (RPD™) file, which empowers the sender with insights and provides peace-of-mind with security. Depending on the level of access controls, the sender can track popularity of a document, track specific reader activity, or restrict access to certain designated viewers – all with no companion software download or logins for readers.

Content Protection: Who, What and When

Senders can make a document self-destruct on a timer, on a specific date, after a number of views, or at the click of a button at the originator – for example, to “unsend” a misaddressed sensitive attachment. RDocs further allows the originator to add dynamic watermarks that are associated with each viewer to discourage unauthorized sharing, or ultimately to track a leaker. Originators can even restrict or track screen captures and printing.

Location, Location, Location

RDocs makes it easy for the file originator to send or generate an RPD™ file and restrict the geography where it can be viewed, make it viewable only for staff inside a company, or define the internet locations where it can be accessed – by reader domain, IP range, or geographic region.

Social Documents, Collaboration Re-Invented

The coolness of social media now meets electronic documents. RDocs has built the power of social interaction into documents. Not only can users track who viewed what, when and where, and for how long, but can also append notes into the document and tally viewers’ votes, likes, and feedback in real time. Users can gauge the popularity of documents in many new ways.

Control Even After the Send

Whether senders later decide that sensitive document probably should not live a full life out-in-the-ether or in their colleague's inbox; or they realize they accidentally sent sensitive content to the wrong recipient, they have total control of their document. Senders can kill the document --- make it self-destruct without trace --- or temporarily disable viewing, and more; all after the send.

Goodbye One-Size-Fits-All, Hello Tailor-Made Security

Delving into more specifics, with the RDocs RPD file converter/generation service, document originators can opt between three levels of security and customize everything from IP range availability to document expiry per viewer, even after the send.

These capabilities can be applied to a document attached to an email, while the email is in transit, or to a file that is converted to an RPD for storage or later sharing (simultaneously submitted as a document and retrieved as an RPD).

Track Views: Level 1 Security

With Level 1 Security there is no requirement at the recipient other than to open and view documents.

Document originators can opt to restrict viewing to certain geographic locations or other internet locations, such as only within their corporate network.

Document originators may additionally choose to protect the content by scheduling a precise document availability, and may apply additional advanced content protections to the document, including:

- Proof of sending,
- Watermarking the document with visible marks,
- Timestamping the original document,
- Print restricting,
- Permitting in-document message responses to the originator,
- Generating authorized reader identity-marking to track a photo-capturing leaker, and
- Killing a document and all of its traces.

A common use for Track Views: Level 1 Security is to be able to have visibility into popularity of a document that may be transmitted or posted for download (number of times viewed, duration of viewing, etc.) and yet retain the ability to, at will, expire viewing for all viewers. This can also be used to create an aura of true urgency to view content before a deadline, for example.

Track Readers: Level 2 Security

Level 2 Security provides the original sender insights into how many times and in what geographic locations the document has been opened and viewed, with insights tagged to each reader.

Readers are identified, associated with their authenticated email address, and insights are displayed to the originator in a web-based activity log, displaying:

- Notification of reading,

- Who read what and when,
- Tracked distribution (forwards),
- How many times the original document was read,
- Time duration of each viewer's reading, and
- Geographic IP location of each reading.

Social Documents

RDocs enables in-document real-time interactivity by allowing the document originator to append notes to a document that are viewed by readers inside the document itself without altering document content, and to carry out reader polls (and tally reader like and dislike votes). Viewers can record their votes, comments or leave questions for the Originator.

Votes are recorded for each tracked reader and are tallied for the originator in a web dashboard visible to the originator so that the originator can easily track and view both the individual votes as well as the aggregate vote tally for each document.

The originator may further choose to permit each viewer to see how others with document access have voted individually and/or in total, or the originator may restrict the vote tally and vote details so that only the originator has view of the vote results.

Leakers Folly

RDocs empowers originators with actionable proof to identify those who disclose sensitive content (or for example, restricted content under non-disclosure agreements) thanks to steganographic, dynamic and in-motion watermarking that is uniquely identifiable to each authorized recipient. Uniquely applied to RDocs, this option can also restrict viewing to the authorized reader's initial reading IP-based geo-location plus can add authorized reader visual identity tags that traverse each viewed page. Readers visually see that if they were to share a snapshot of any one page or part of a page, they would be at risk of the leak being easily traced back to them. As a result, RDocs not only discourages unauthorized sharing, but can further provide court-admissible proof of who shared any unauthorized snapshot of a document.

Targeted Marketing

RDocs enables originators to be able to track who is reading their content, even after the first person accessed it.

For example, today, many reports or other content is posted for download, accessible after a form fill or a log-in to an intranet. Normally, the originator loses control of the content and visibility as to who is interested in the content enough to read it "secondhand" after an initial viewer downloads and shares the content. With RDocs, content originators can gain visibility of who is reading their content along with the secondhand readers' email addresses. Armed with this information, originators can expand their lists of who is interested in their content beyond their current list of "firsthand" readers and carry out marketing outreach campaigns accordingly.

Restrict Readers: Level 3 Security

Restrict Readers: Level 3 Security provides the original sender all the controls and insights of Track Readers: Level 2 Security, plus additionally allows the originator to restrict specifically who can read the document.

Readers are tracked and restricted to only those pre-authorized (or a pre-set list of authorized readers). Two-factor authentication assures the reader associated with their email address is in fact who the originator has authorized to access the RPD file.

Additionally, Level 3 Security provides an extra layer of protection by allowing the document originator to:

- Restrict viewing of the document to a registered viewer or list of registered viewers, and
- Restrict forwarding (distribution) of the document by registered viewers.

Example Use Cases

Some examples of high value content distributed as PDF files that would better serve the originator if distributed as RPD files include research reports and financial tip newsletters; non-public corporate, board or shareholder reports; funds transfer information; invoices; final versions of agreements related to highly sensitive transactions.

Each of these (and other) documents would be better served as an RPD, with different feature sets or access levels depending on the type of document or desired document-centric functionality.

Type of Document	RPD Security Level	Other RPD Features	Main Benefit vs. PDF
Research reports, financial tip newsletters, real estate market reports, subscription content	Level 3: Restrict Readers	ID Leakers, watermark, timestamp, expire on a timed schedule or after a number of views.	Prevents distribution to unauthorized viewers, protecting content license revenue.
Research reports	Level 2: Track Readers	ID Leakers, Watermark	Gather email addresses of “secondhand” viewers for future marketing and re-targeting.
Sales & Marketing content (product roadmaps, reseller battlecards, reseller price tables)	Level 2: Track Readers	Document time availability, IP restriction, reader domain restriction.	Allows sharing of content with controls to limit exposure of sensitive or strategic content to only intended recipients or those within their companies.

Sales & Marketing content (whitepapers, product brochures)	Level 2: Track Readers	Document time availability, voting, notification of reading	Allows to track who is reading what, when, how many times and for how long; capturing popularity of content at the document-level and creating marketing lists with secondhand tracked readers.
Funds transfer information, purchase orders, and invoices	Level 3: Restrict Readers	IP range restriction and domain restriction, notification of reading	Prevents unauthorized viewers, limits wire fraud or the potential of fake invoices.
Non-sensitive internal documents and presentations	Level 1: Track Views	Watermark, document availability	Keep track of how many times and where your documents are accessed, providing insight into document popularity. Expire old presentations and brochures when new ones are available to limit use of outdated material.
Corporate board or shareholder minutes or resolutions	Level 2: Track Readers	Voting, Watermark, ID Leakers	Easily compile votes affirming acceptance of minutes or resolutions, with a tally aggregated conveniently for the originator. Disable access to the file after the vote for privacy.
Technical bulletins (release notes)	Level 1: Track Views		Make sure that these documents are read.
Technical documenatation (software, pharmaceutical, etc.)	Level 1: Track Views	Custom document availability	Kill outdated information.
PII in general	Track Readers / Limit Readers	Watermark, ID Learkes, Custom document availability	Prevent data leaks. Automatically kill content after predefined timeframe.

Conclusion

The post-pandemic world has accelerated the future of work, and a future with focus on decentralization. As a result, technologies that were once revolutionary and full of possibility can no longer keep up with the new ways of doing business. Content shared only within office meeting and board rooms is now accessible out in the ether – often lacking same controls afforded in a controlled environment.

RDocs eliminates the need to control the environment and puts those controls right into documents themselves – protecting and controlling in the now and in the future at the originator’s whim.

As such, being able to share information securely while safeguarding digital rights, digital lifespan, and digital footprints of who is viewing what content and when, and retaining controls, has never been so crucial.

Welcome to the new dawn of Digital Rights Management for documents; the next generation of Portable Document Format (PDF) will be Rights Protected Document™ (RPD). Welcome to the new age of ubiquitously accessible (yet access controlled) **RPD**™ files.