Please fill in the name of the event you are preparing this manuscript for.	2020 International Petroleum Technology Conference
Please fill in your 5-digit IPTC manuscript number.	IPTC-19890
Please fill in your manuscript title.	Digitally Securing and Automating the Distribution of Critical Petroleum Documents

Please fill in your author name(s) and company affiliation.

Given Name	Surname	Company
Hussein	Huwaidi	Saudi Aramco
Noufel	Awami	Saudi Aramco
Irfani	Saifuddin	Saudi Aramco
Walid	Kaskas	Saudi Aramco

Abstract

Objectives/Scope:

A descent percentage of oil and gas content come in digital forms such as documents. Depending on what information they contain, different security is applied. Yet, there is a need for sharing content even when it is critical, although once shared, data managers lose control over it. In this paper, we will show how we managed to automate the digital distribution of critical documents while maintaining control over it even when it reaches the end-user.

Methods, Procedures, Process:

This solution implemented in-house for digitally distributing critical content internally while maintaining security measures without hindering the user experience. It is composed of four parts, namely a repository, a data management tool, a webservices layer and a web-viewer. The repository stores and encrypts the content. While the data management tool allows data managers to interact with the repository and tag the content. The webservices layer audits, puts a watermark, delivers the report securely to end-users that prevents them from saving and/or copying the content. The integrated web-viewer provides a secure way for viewing the content by the users.

Results, Observations, Conclusions:

First, the content is stored encrypted and tagged with recipient's positions and type of data. Depending on the content classification, it either encrypted or stored in a normal storage space. By default, the permission on the document is set such that apart from the author itself, all recipients permitted to view the tags only. Second, the data manager requests a distribution of the content from the system. This triggers an email with all the user email addresses filling the positions tagged as recipients. Third, users receive the email with a secured link to the content. When this link accessed, a secure web-viewer opens on the recipient machine, which sends a request to the webservices layer for viewing the content automatically. If the recipient allowed access to the tags, escalated privileges used to temporarily obtain higher level of access on the document content, a watermark is applied with the recipient identification and sends back to the web-viewer that renders the content on the browser without downloading on the workstation. This web-viewer adds additional security restrictions and allows specific features requested by the data managers such as not allowing copying, not allowing downloading, but allowing searching and printing.

Novel/Additive Information:

This solution replaced manual process of fetching position holder emails, the distribution of the content through emails and only allowing viewing the content through the secured web-viewer. Thus preventing leakages from creation of the document, to storing on the repository and securely delivering it all the way to the recipient. This eliminates the need for making multiple copies while keeping control of who can view the content and for how long.