RPX Projects

1. T Session -1

Date : 30-Sept-2018

Resources : Payani Putturu, Dinesh Singaram

RPX OVERVIEW

1. Resolves patent related disputes.
2. Non Practising Entities(NPE)-C6 Group of companies which make profit from illegaal activities by simply filing a case against those who are using patents without license.
3. RPX -They buy license from patent owners(either ownership or sublicense), save it in their databases and if any litigation related with patents occurs they support their registered clients so that cost and risk get reduced for the clients.
4. Taking data from USPTO using PACER which can be in any format.
5. Terminologies used in RPX
   1. Plaintiff - patent owner
   2. Defendant - who used patent without license
   3. Litigation - Cases or dispute on some patents
   4. Entity/aliases - Company/judges/lawyers or anyone involved in litigation Internal Applications
6. Main goal of internal app is to verify or validate the data from the external source(UPSTO) and delivered to insight applications.

PROJECTS

1. Internal Applications

There are Four Internal applications(projects):

1. Data Managing Application(DMA)
2. Acquiflow
3. Member Credit
4. Docblaster
5. DMA (Data Management Application)
6. Focussed on verifying data based on litigation and aliases.
7. Work flow- External source(USPTO-PACER) -> OCR -> cordDB -> DMA\_app -> cordDb ->cortalDB -> Insight Application/Internal Apps.
8. OCR processor extract the information related to plaintiff, descendant etc from the pdf file.
9. The data obtained from OCR is stored in cordDB in DMA\_app.
10. In DMA\_app all the corrections are made and also mapping between entities/aliases are done.
11. Mapped data is send to cordDB, through ETL only correct data is given to cortalDB
12. The final verified data is accessed by insight applications.
13. Acquiflow :
14. Deals with Acquisition
15. Acquisition : Getting patent Data from source (NPEs) and grouping it in a form of portfolio
16. Portfolio consists of group of patents where each groups is specific to any particular industry.
17. Encumbrance : Tracking of patents to whom provided licence and providing any kind of restrictions for usage
18. Indication : Contribution of RPX with any other party which is interested to buy same licence in partnership.
19. Member Credits :
20. This is only for internal purpose to display how much an RPX member got credit.
21. Member credit will fetch all the data related to payments, contracts, memberships to calculate the credit
22. Docblaster :
23. PTAB : Patent Trial Appealed Board where some other entity file a case claiming that the patent is own by them.

KT Session -2

Resource : Abdul Rafiu

Date : 3/09/2018

PROJECTS

1. Authenticator
2. Patent Document Service
3. Authenticator :
   1. Authenticator provides Single-Sign On service for all Apps(Insight, Analyst, Internal Apps)
   2. Project has been done by overriding OAuth architecture
   3. O Auth : Open Standar Authorization describes how unrelated servers and services can safely allow authenticated access to their assets without actually sharing the initial, related, single logon credential.
   4. OAuth Example : sign in via google or facebook to any application

Explaination :

1. The first website connects to the second website on behalf of the user, using OAuth, providing the user’s verified identity. And it will check for the cookies for session key and access token if session key not present then
2. The second site generates a one-time token and a one-time secret unique to the transaction and parties involved.
3. The first site gives this token and secret to the initiating user’s client software.
4. The client’s software presents the request token and secret to their authorization provider (which may or may not be the second site).
5. If not already authenticated to the authorization provider, the client may be asked to authenticate. After authentication, the client is asked to approve the authorization transaction to the second website.
6. The user approves (or their software silently approves) a particular transaction type at the first website.
7. The user is given an approved access token (notice it’s no longer a request token).
8. The user gives the approved access token to the first website.
9. The first website gives the access token to the second website as proof of authentication on behalf of the user.
10. The second website lets the first website access their site on behalf of the user.
11. The user sees a successfully completed transaction occurring.
12. Single Sign On :
    1. user [logs in](https://en.wikipedia.org/wiki/Login" \o "Login) with a single ID and password to gain access to a connected Application or Application without using different usernames or passwords.
    2. In other words sharing the credentials to all connected applications such that every time user don’t have to login for each application.

.