Partner case

Login authorization control

Background / Problem statement:

In the oil and gas industry drilling service suppliers provide its clients a possibility to monitor and receive real time drilling and geology data from a remote drilling rigs using so called Real time data system. It is a web based service with servers in Moscow that provides important tool for an informed and fast decision by the Client in his own office in town, without the need to wait for the geology or drilling data from the wellsite to be sent via email or other means. Realtime data system is working with highly sensitive and confidential client data which is a reason why a system of Login authorization and designated Client folder access management is in place. Each registering and applying for an access to client data user is granted permission only after a responsible client representative authorizes him. After user is granted permission to access the Client folder in Realtime data system, data supplier does not have any means of controlling whether it is this particular user logged in to interact or someone else obtained his Login/password and use it to work in the Realtime data system. There are 2 factors to consider: 1) Realtime data system provides Clients possibility to use service from both personal laptops and mobile devices, like tablets or smartphones, meaning that user can use his Realtime data system login/password on lap top and mobile device at the same time; 2) If multiple Realtime data system users are working from their desk in the Client office, all the PC's are often recognized under one static IP because all of them are using the same device as a bridge.

Task:

Main objective is to gain possibility and technology approach how to control who is using Login/Password and that it is not passed to other person for use without Realtime data system Team notice. Ability to identify simultaneous use of individual Login/Password.

Solution requirements:

A PowerPoint presentation, describing the possible solution, required resources, its pros and cons, timeline required and possible legal constraints (if known).

Technical requirements for the solution:

There is no strict formal technical requirements for presentation. Main requirement is clearness of solution and instruments used/required to deploy.

Evaluation criteria:

- Criterion: Reliability and precision of identification of use of individual Login/Password (both over closed networks via gateway and when parallel use of PC and Mobile/Tablet)
  Evaluation: maximum 5 - minimum 1.
- Criterion: Ease and cost of implementation
  Evaluation: maximum 5 - minimum 1.
- Criterion: Original approach
  Evaluation: maximum 5 - minimum 1.
- Criterion: Possible legal constraints
  Evaluation: maximum 5 - minimum 1.