

# Secret vault implementation challenges

**Václav Šamša**

KeyShield & SecureAnyBox





# Agenda

- Why Secret Vault
- What is a Secret Vault
- Secret Vault technology
- DEMO
- Q&A



# Why secret vault?

- Yet another nice word, like cloud
- The different word underlines the difference
  - compare File\_System x Secret\_Vault. What sounds better?
  - the different word works even if there is NO difference
- The goal is to convince people (users) to trust
- If people do not trust then they simply do not use
  - regardless of the money you spent on the new shiny thing
  - regardless of the efforts you did invest into implementation



# What is a Secret Vault?

- There is no technical nor commonly accepted definition of a Secret Vault
- The same situation like with yet another promising word – car. In some parts of the world, homemade four wheels something without brakes is called a car. Such car is not allowed to use public roads in other parts of the world.
- But there is an official agency approving cars to use public roads. Such agency is generally trusted (sometimes by law :-))
- In IT – you can trust whatever you want



# What is a Secret Vault?

- Any proud member of the IT crowd can trust something called a Secret Vault. If you administer it, you trust it because you trust your great job
- Does it mean that users trust it too?
- No. Not at all. Users do not trust their own administrators
- If you are not able to convince your own users to trust, then you do not have a Secret Vault
- The opposite to a Secret Vault is data on local drives, mobile phones, clouds, browsers and other horrible places



# Secret Vault technology

- Some file systems are pretty secure:
  - encrypted whole hard drives
  - encrypted drives (partitons or so)
  - encrypted data transfer in between the client and the system
- OK, where is the problem? How the access is granted
  - if it is a meta-data based, it is not secure. Sorry.
- Want to learn how secure is something you are thinking about? Try to find something like “Administrator will give access to the user“ in the documentation
- If this is the way how it works, it is not secure. Unless you are the Administrator and the only user (the only employee)



# Secret Vault technology

- The only secure technology is encryption. OK, but what is the difference?
  - if the system has the keys, anybody administering the system can do anything
  - If the users have the keys, only key owners can do something
- OK, you agree, you knew this before this boring session did start. And?
- I'll show you in the DEMO part how our implementation works
- But still – how to convince the users?
- Our proven way is to provide the users with relevant information
- I'm in love with GroupWise for roughly 25 years. Do you remember what it does when you try to put a document in a folder where somebody else has access?



# Secret Vault technology

- Yes – GroupWise shows a pop-up telling you: if you do it somebody else will get access to your document
- GroupWise team, some of them are my distant (US is far away) friends for long time, is thinking in exactly the same way as us
- Imagine yourself having your valuable secrets and being pushed to move them into the organization Secret Vault. Tough moment, isn't it?
- The first you want to get is a feeling
- If the door looks secure enough, who else has the key?





# Secret Vault technology

- Be open and show the users what can convince them:
  - who else has the key
  - what the other users can do
  - what is recorded in the audit
  - let them use notification
- If there is a back door to the user's private data, let them know who and how can open the back door
- Do not use account names like Administrator, root, admin, consultant etc.
- Secret Vault should control access to such privileged accounts but privileged accounts should not have access to secrets
- Mr Smith and Mrs Doe should be the names, the real names, who can access secrets = own some instances of the keys



## DEMO time!

- SecureAnyBox does what we believe is the best for anybody who wants to keep, share and use secrets in a safe way
- Let's take a look

# Questions & Answers

Václav Šamša

KeyShield & SecureAnyBox

vsamsa@tdp.cz

