RushFiles Architecture and Security

RushFiles current Architecture and Security

July 2021

www.rushfiles.com

Contents

1. RushFiles Architecture

1.1 General setup

Currently RushFiles offers to partners two types of setup: a general setup and an Isolated Data Island setup.

In our Overview of the RushFiles Architecture (Figure 1) we show the following elements:

- **RushFiles APPs**: the applications offered by RushFiles for your users to share files
  - 2 desktop versions: one for Windows (PC Client) and one for Mac
  - 2 mobile versions: one for iOS and one for Android
  - Web Client, can be accessed using any browser

  RushFiles offers our partners the possibility to white-label RushFiles applications so that their branding elements (eg. Colors, application name, logo) match the partner's brand, and make the client "their own".

- **Auth.RushFiles.com**: Central component owned by RushFiles. Acts as a federation gateway for other identity providers (e.g. domainauth). Allows SSO (Single Sign-On) across multiple domains.

- **Domain setup**: represents a partner installation performed on their servers. On these servers, partners will have:

  - IIS to host your Web Client and our API services:
    - Client Gateway
    - Domain Master - responsible of database management
    - File Cache – perform operations on files (upload, download)
    - **Domain Auth –** local IdentityProvider & Authorization server, SSO endpoint for all client applications
  - Windows Services for maintenance purposes
  - RushFiles DB – Mongo database (can be installed on a Linux server)

- **Domain Auth**: Identity Provider component handling the authentication of users in the system. This identity provider can be extended by integrating with other Identity Providers like ADFS (Active Directory Federation Services) or other Enterprise Identity Providers that implement OpenIDConnect and OAuth. OpenID Connect 1.0 is an identity layer on top of the OAuth 2.0 protocol. It allows identity validation of the user based on the authentication performed by an

Authorization Server, as well as to obtain basic profile information about the user.

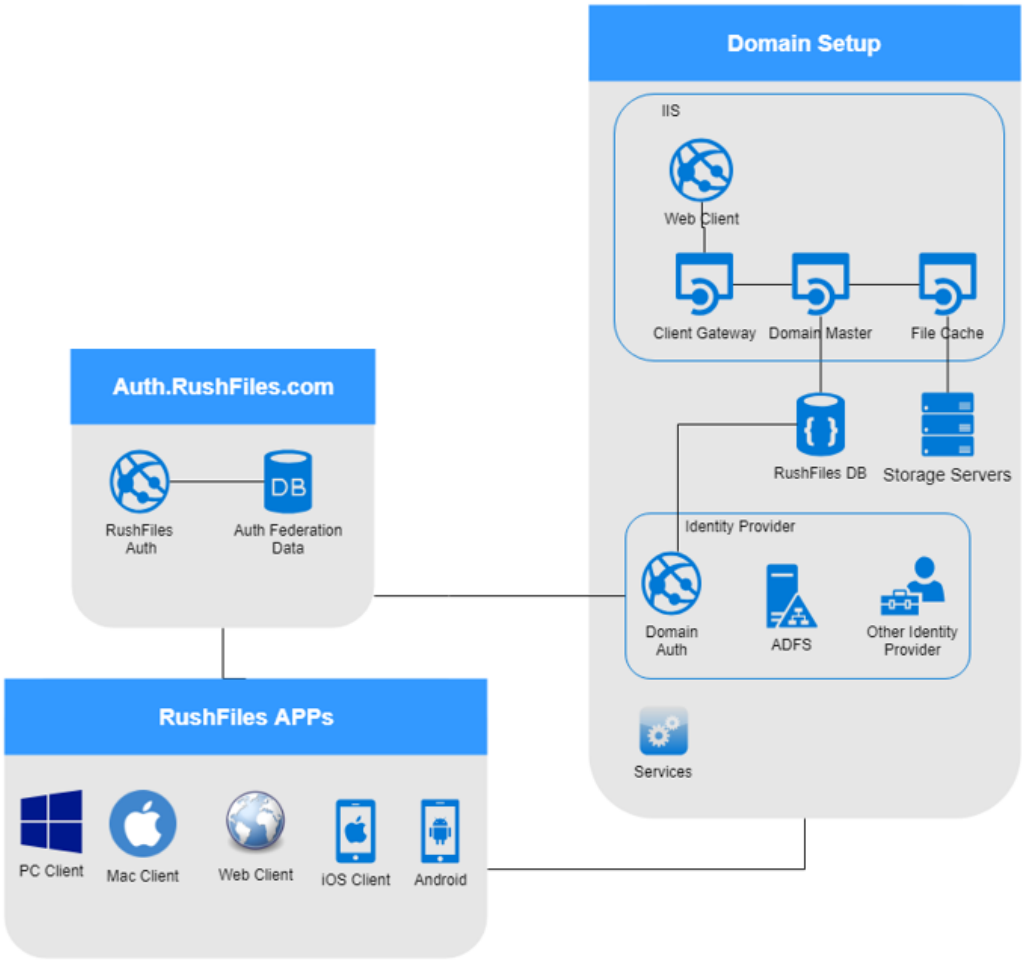

Figure 1- RushFiles Architecture Overview

RushFiles is designed to allow users to login using Single Sign-On (SSO) by connection to multiple domains (server installations). The Auth.Rushfiles.com component enables access to multiple servers from the same client application.

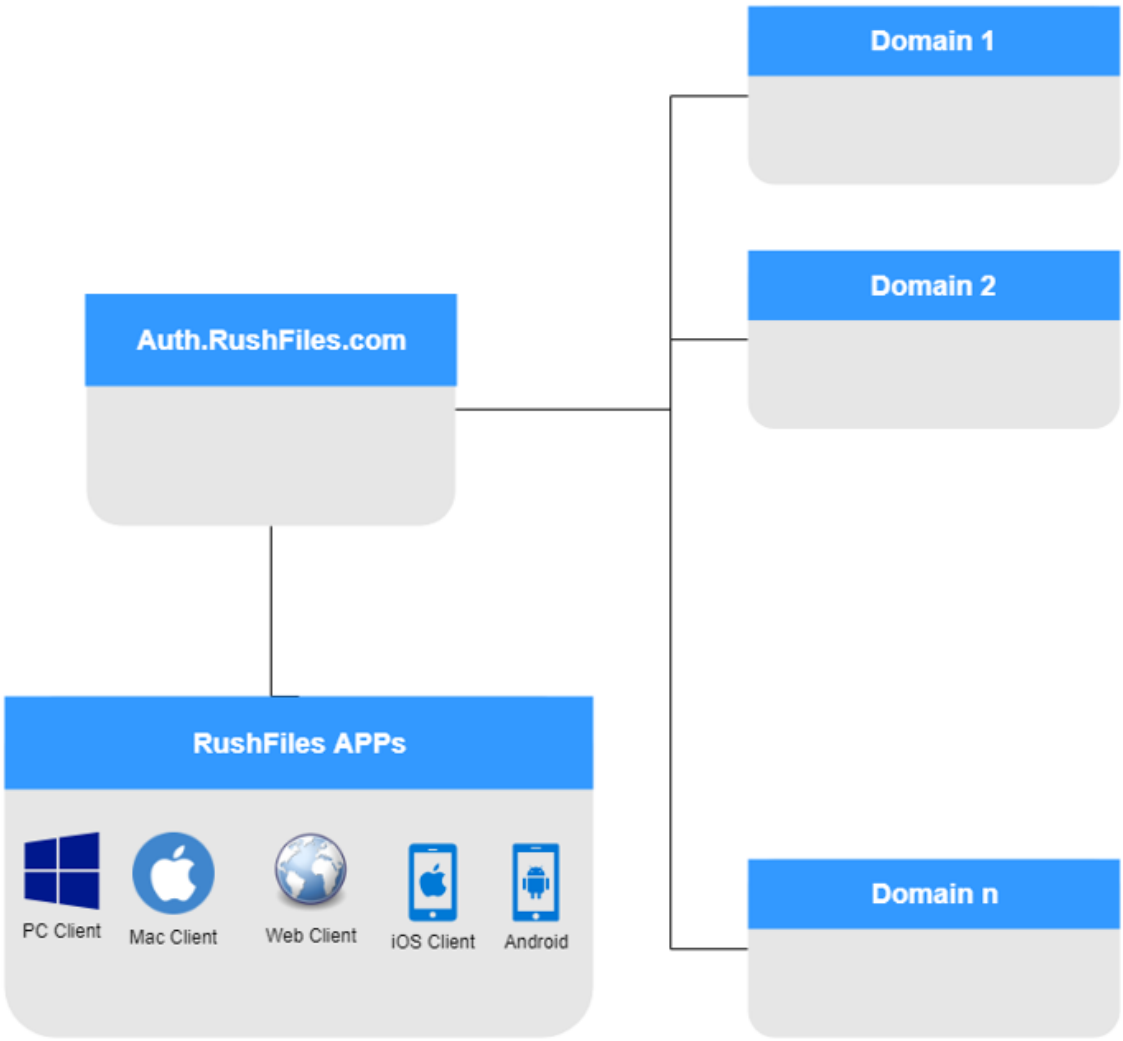

Figure 2 - Multiple Domain Login with Auth.RushFiles.com

The Auth.RushFiles component automatically forwards the user based on the email address to the primary domain where the user belongs to. After entering the password, the Domain Auth component on the primary domain validates the user's credentials providing a token. This token is returned to the client application together with the list of domains the user is assigned to. The token can be used by the client applications on all domains to gather information (see Figure 3).

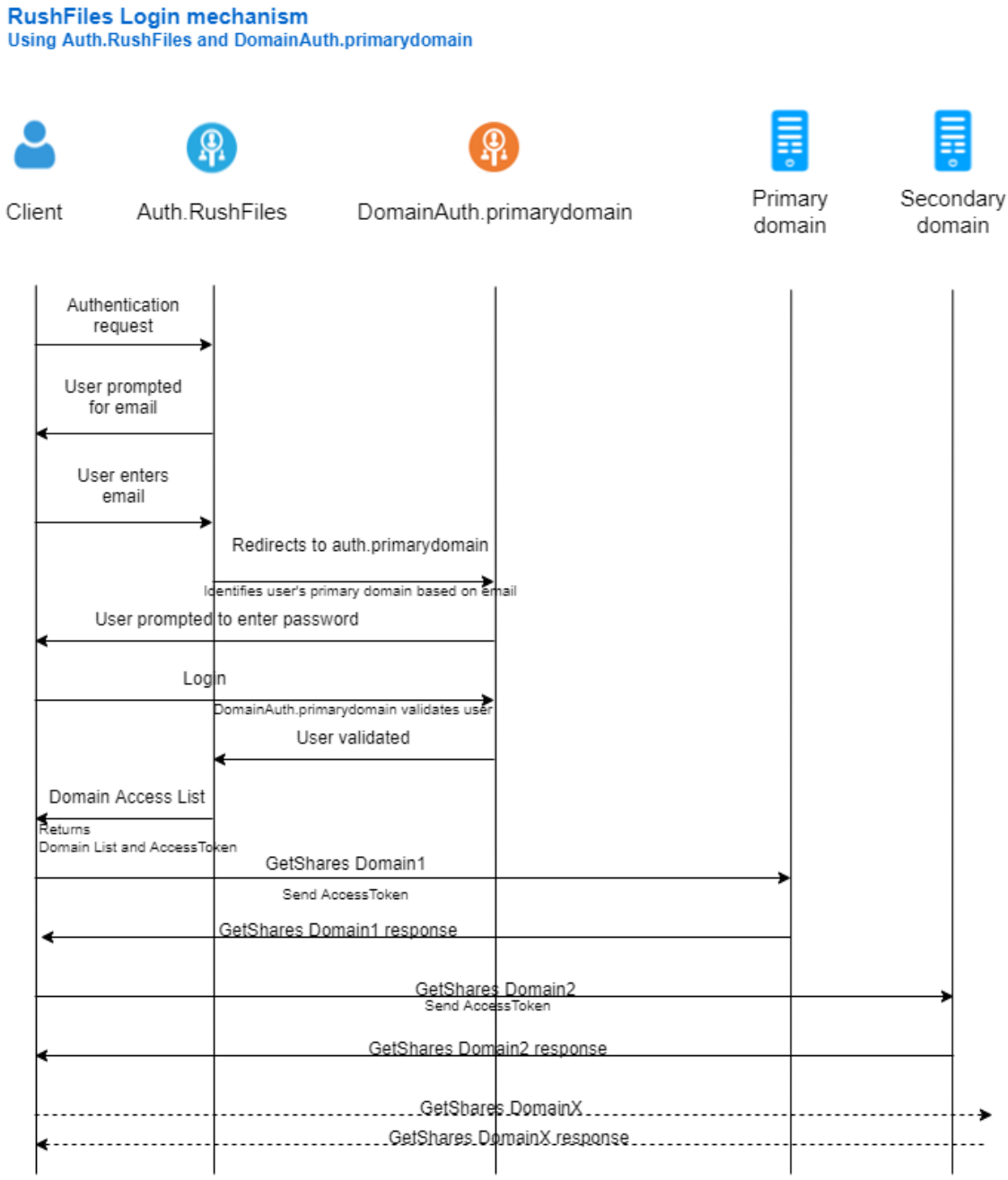

Figure 3- Login mechanism with Auth.RushFiles

1.2 Isolated Data Island

Isolated Data Island is a high security version of RushFiles offered to our partners. In this setup, all communications are done inside the network, with no interaction with external components, except for interacting with our WOPI (Microsoft Office Online) integration. However, the use of the WOPI integration is completely optional.

This type of setup is often used if the end-users are part of financial institutions or other types of institutions that require high level of security.

Data Island requires white-labelled client applications that target your domain URL, meaning that users will need specific, white-labelled client applications to access their data.

The Identity Provider component enables SSO for this setup as well. Domain Auth is the primary Identity Provider used for user authentication with the extensibility option though integration with other External Identity Providers.

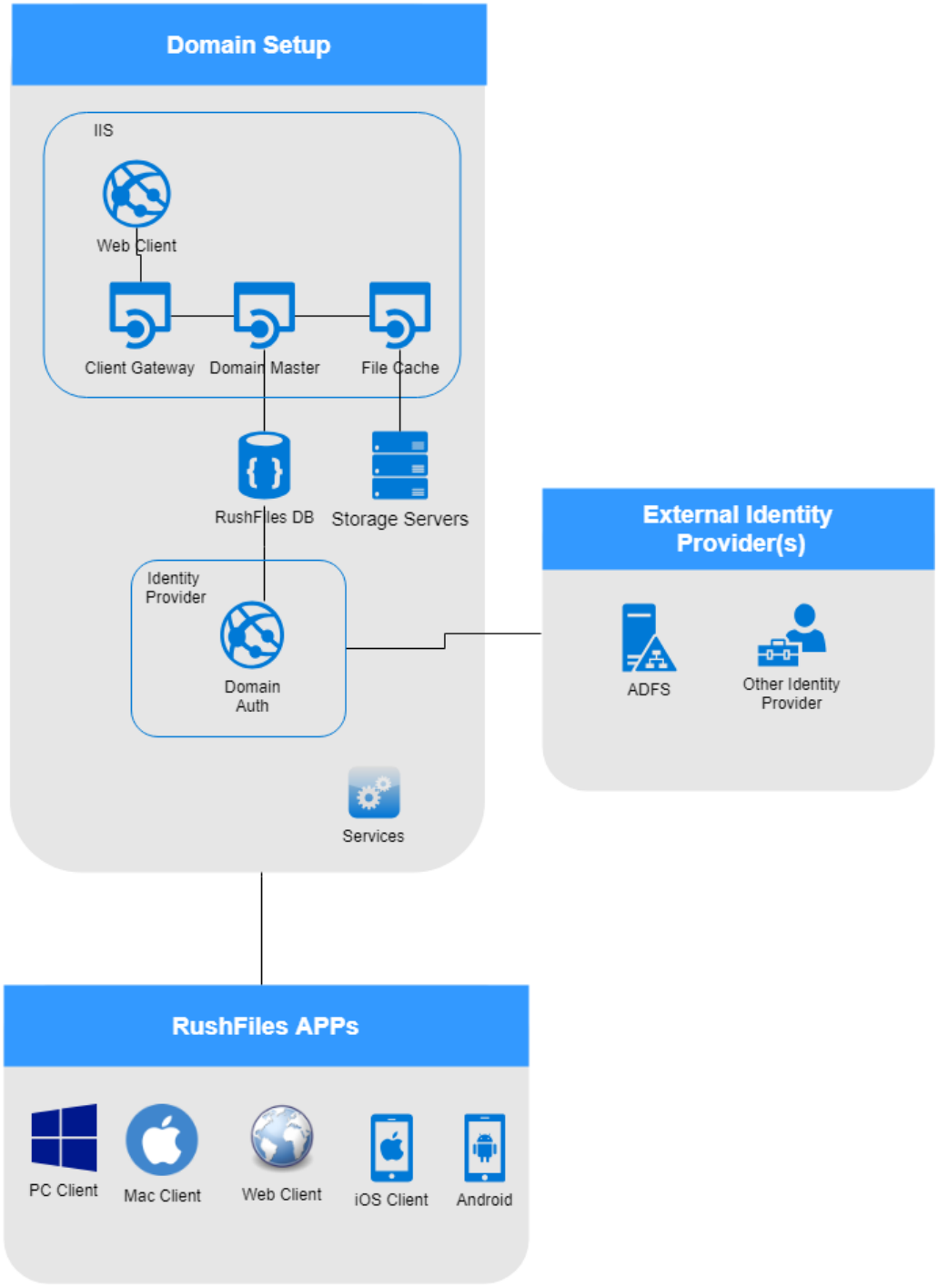

Figure 4- Data Island with Domain.Auth

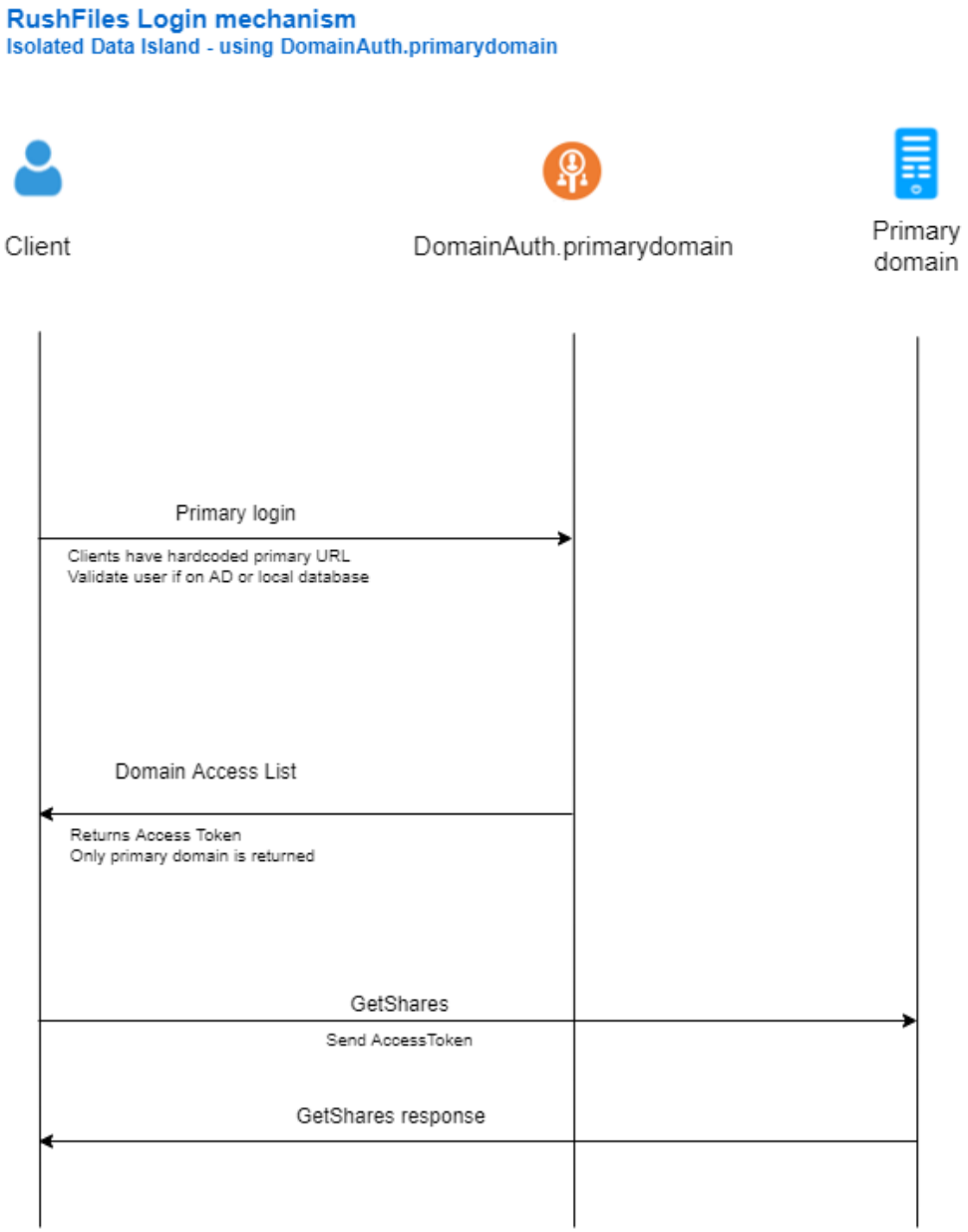

Figure 5- Login Mechanism using Domain.Auth for Data Islands

2. Security features

2.1 Secure communication

All communication in RushFiles is done based on Secure SSL communication on port 443.

The RushFiles applications only support SSL Certificates that are digitally signed by a trusted CA (Certificate Authority). This prevents the use of SSL proxy to perform “man in the middle” sniffing of the data traffic.

It is up to RushFiles’ partners to install the certificate on the server running the RushFiles services and RushFiles recommend use of minimum 2048-bit wildcard certificate signed by a trusted CA.

2.2 File encryption

All files are encrypted on our servers. All files are encrypted using AES (Advanced Encryption Standards) with a 256-bit key. AES is a symmetric block cipher chosen to protect classified information and is implemented throughout the world to encrypt sensitive data. We use private generated keys for each of the companies using RushFiles.

2.3 Obfuscation of data on partners servers

All file and folders are obfuscated by not using the original name and mime type, so files cannot be discovered. Additionally, the file and folder structure are secured in a database and the files are not stored in the same structure on disk to obfuscate them even more.

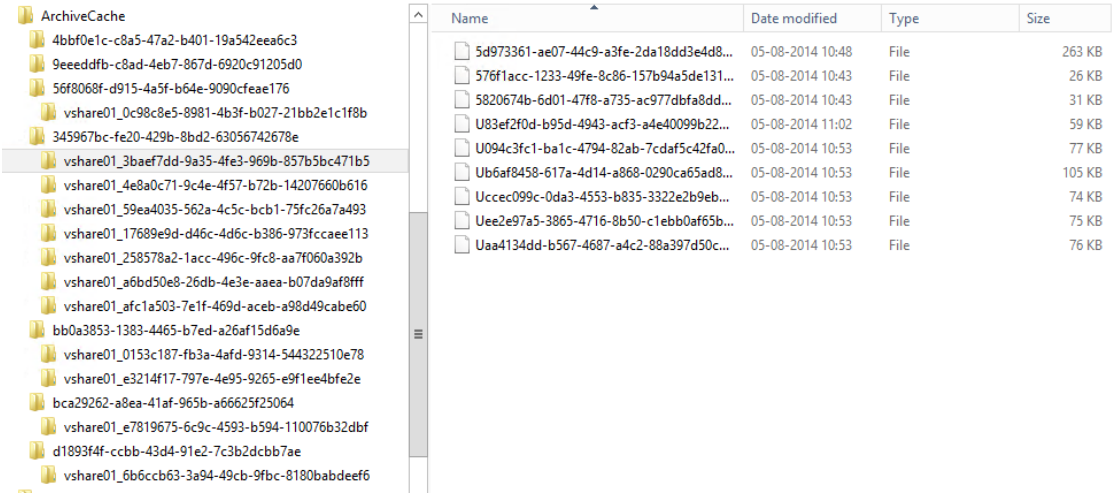

Figure 6 - Example of obfuscated files on server

The purpose of encryption at the server level would be to prohibit the server administrator from accessing the files' contents.

2.4 Credentials

RushFiles can be accessed and used by users within a company account. Companies have the option to integrate their existing Active Directory (AD) with RushFiles, but can also create users into our system.

Password security if use of AD integration

For users set up to use AD, their password is only stored in the AD and the password rules that apply in the AD are enforced since RushFiles always authenticates the user credentials through Single Sign On (SSO) directly in the AD.

Password security without AD integration

If the organization does not have AD integration, the standard RushFiles password security rules apply and the password must be strong, meaning:

- Minimum 8 characters
- Upper and lower letters are required
- At least one numbers are one special character is required

However, the password constraints can be customized by Company administrators, and then these custom constraints apply to users of that specific company account.

Only the individual user can change the password by requesting a one-time link sent to the email address the user is registered with. Company administrators have the option to resend the reset password email but cannot set the password for their users.

The authentication of users is handled on the Primary domain of the user, using Domain Auth acting as an Identity Provider. The Auth.RushFiles.com component is in charge to redirect the users to the primary domain the user is assigned to. Auth.RushFiles.com component stores information regarding the list of domains where the user is assigned to.

Login using AD and other Identity Providers is handled on our partner's servers.