RUSHFILES ARCHITECTURE AND SECURITY

RushFiles current and ongoing Architecture and Security

April 2019

www.rushfiles.com

Contents

1. INTRODUCTION

This document describes the available architectural setups and security features offered by RushFiles solution. It also serves as a reference for partners when addressing customer's queries on possible setup and security.

2. ARCHITECTURE

In this section, we will present the current setups offered by RushFiles for our partners, but also some improvements and ongoing changes to our Architecture.

2.1. Current Architecture

2.1.1. General setup

Currently, RushFiles offers two types of setup to partners. This includes a General setup and an Isolated Data Island setup.

In our Overview of RushFiles Architecture (Figure 1), you will see the following elements:

- **RushFiles APPs** are 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 for iOS and Android
  - Web Client, the version that can be accessed using any browser

  RushFiles offers our partners the possibility of rebranding RushFiles applications as their own client applications.

- **Global** this is a central component owned by RushFiles. This component acts as a Licensing platform and as an SSO (Sign Sign-On) central component.

- **Domain setup** represents a partner's installation of RushFiles on their servers. On these servers, partners will have:

  - IIS to host your Web Client and our API services:
    - Client Gateway
    - Domain Master – responsible for database management
    - File Cache – perform operations on files (upload, download)
  - Windows Services for maintenance purposes
  - RushFiles DB – Mongo database (can be installed on a Linux server)

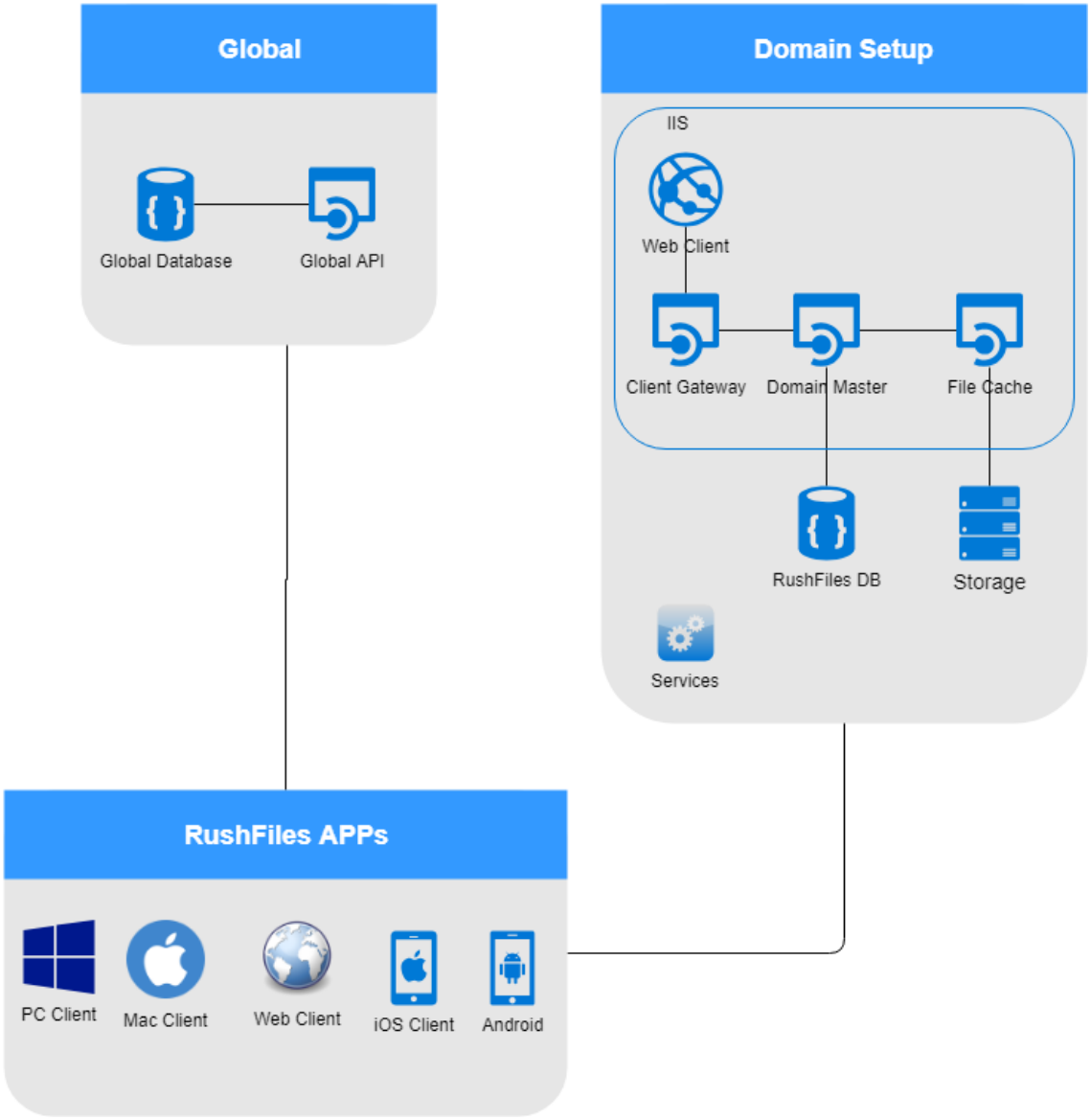

Figure 1- RushFiles Architecture Overview

RushFiles is designed to allow users to login using Single Sign-on (SSO) by connecting to Multiple Domains (server installations). Our Global component enables access to multiple servers from the same client application.

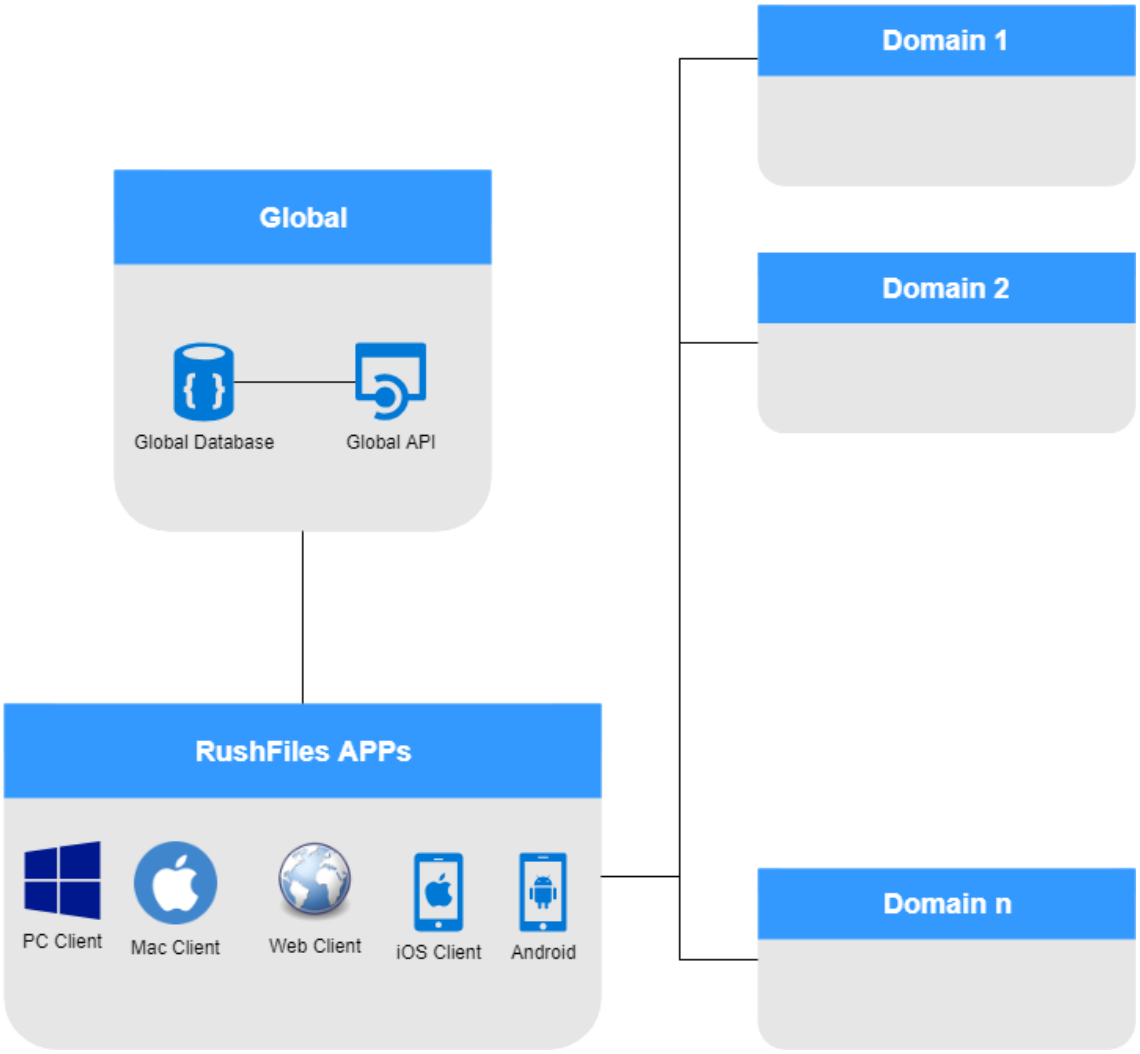

Figure 2- RushFiles Multiple Domain Login

In order to perform Multiple Domain login, our client applications interrogate our Global component to return the primary domain of the user. The primary domain of a user is the domain where a user was initially created. After obtaining the primary domain, the user is validated on the primary domain setup, which returns a list of domains and tokens that the user can access. With these tokens, the client applications can obtain information from each domain. Below, you can find a diagram exemplifying our login mechanism and how the client applications gather information regarding user shares.

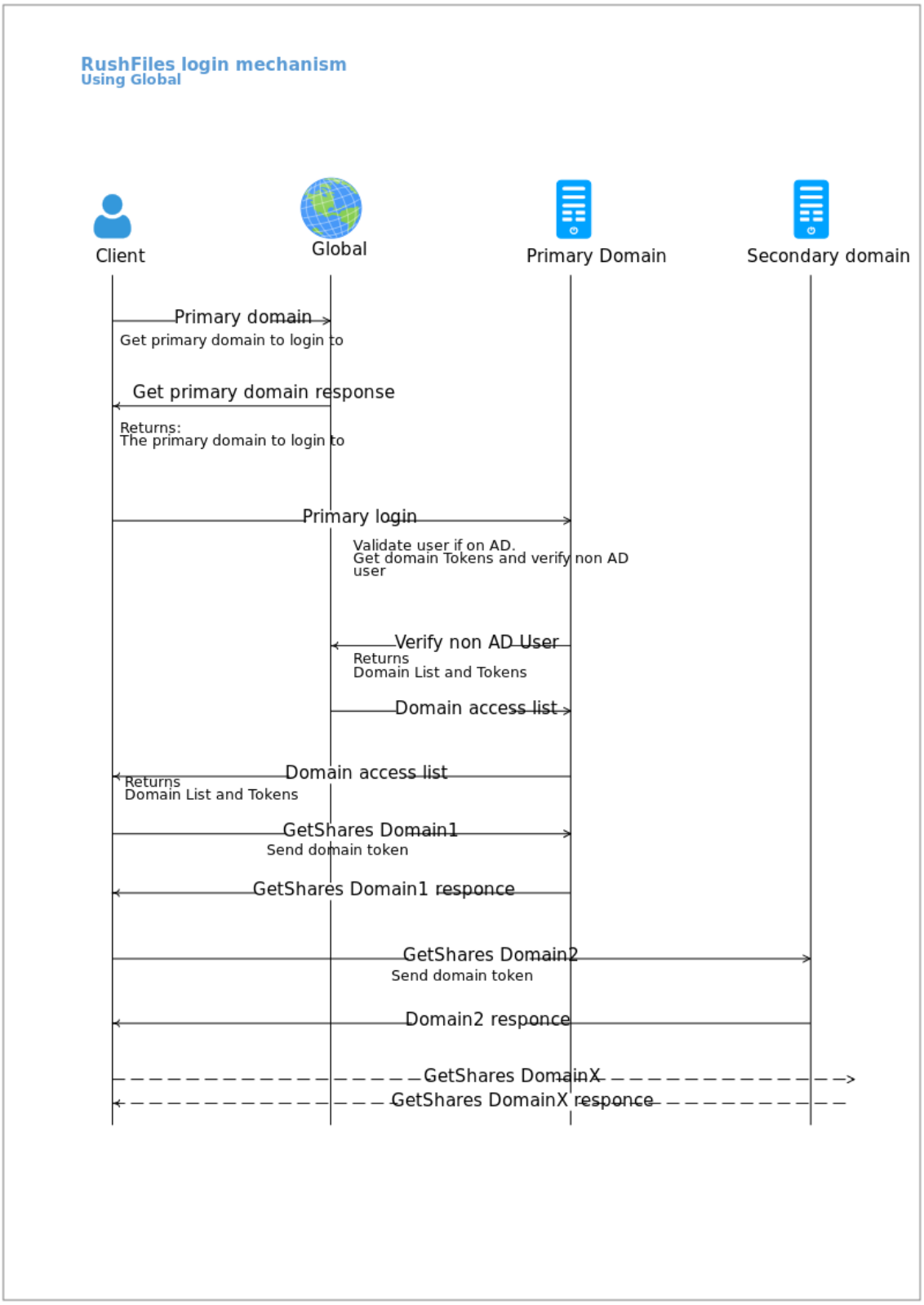

Figure 3- Login Mechanism using Global

2.1.2. Isolated Data Island

Isolated Data Island is a setup which offers our partners a way to separate their local installation from an external network. This way, we ensure that private and sensitive data is stored and guarded inside your network.

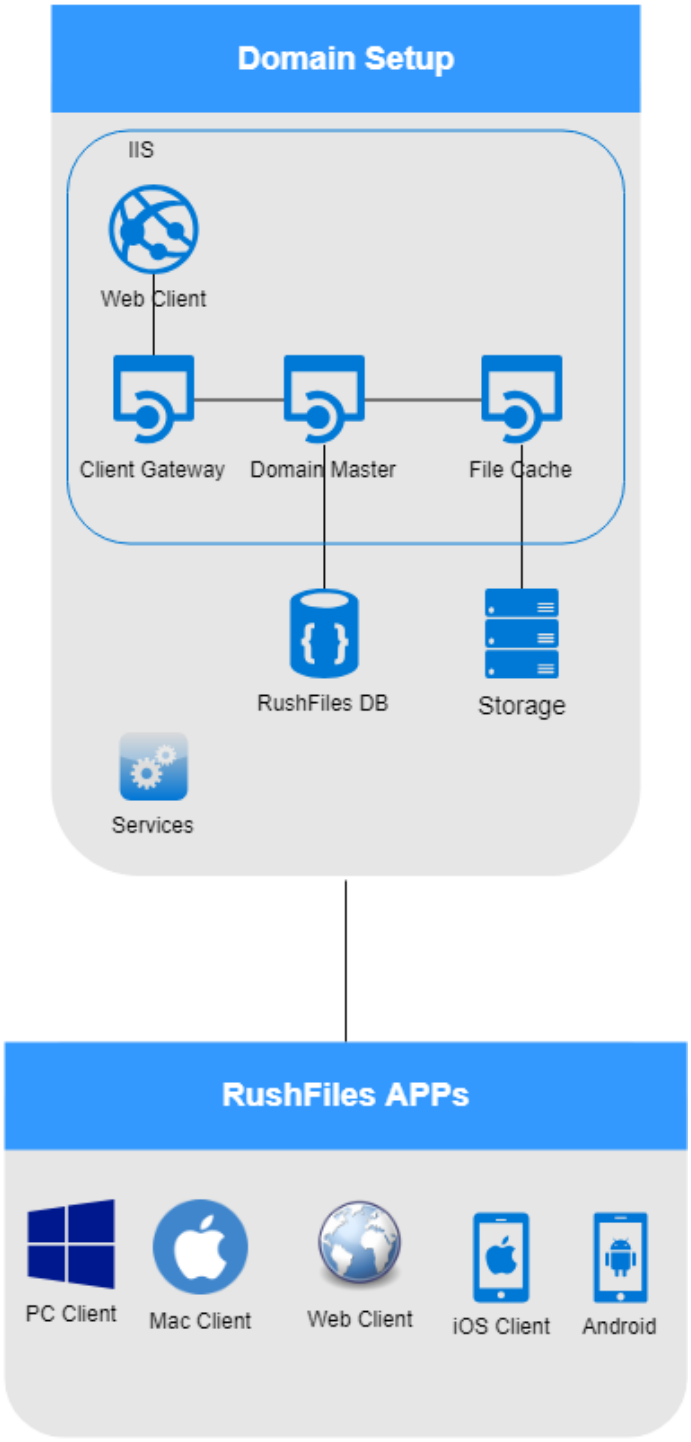

Figure 4 Isolated Data Island Setup

In this setup, communication with our Global component is bypassed, thereby ensuring that all data is stored inside your Domain Setup. Multiple Domain login is not possible, instead, the users are assigned to your company's domain. Below, you can see an image of how the login mechanism is implemented for this setup.

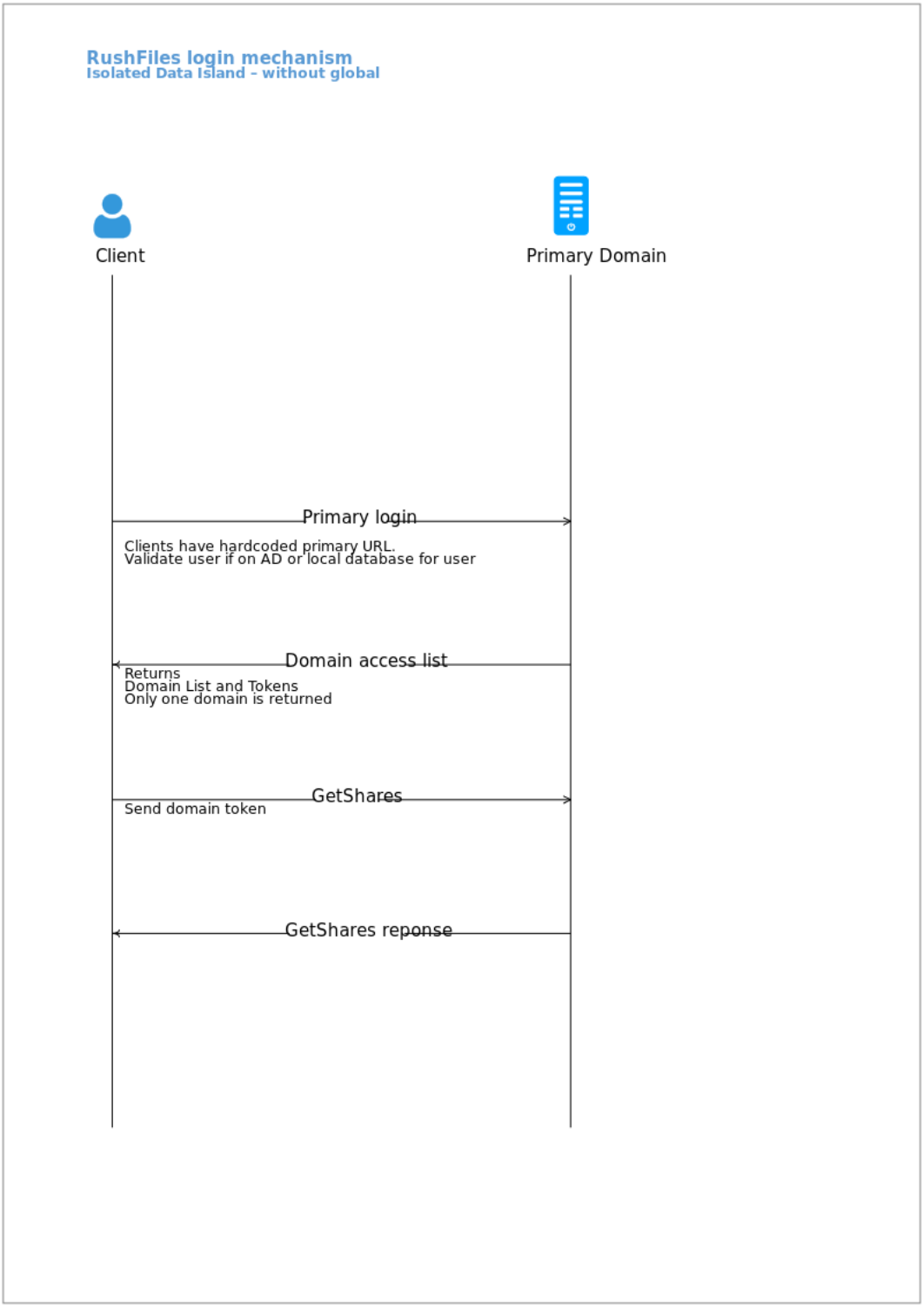

Figure 5- Login Mechanism on Data Islands

2.2. Proposed Architecture changes

2.2.1. General setup

We propose changes to our current architecture in order to extend our Single Sign-On (SSO) and enable partners to integrate with several External Identity Providers by introducing the following components:

- **Auth.RushFiles.com** – Identity Provider component acting as arbiter for users' authentication. This component stores the list of domains the user is assigned to and identifies the primary domain on which the user is validated
- **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.

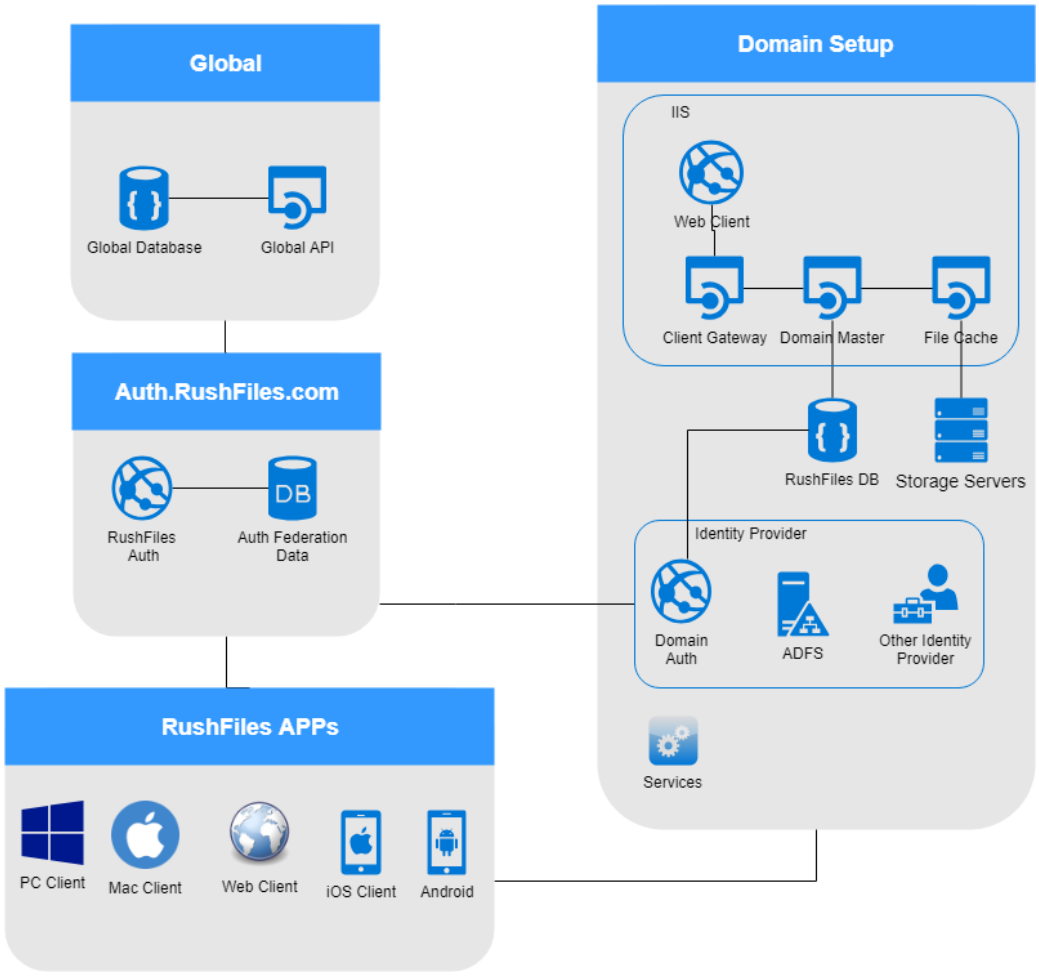

Figure 6- Introduction of Auth.RushFiles.com

RushFiles will maintain the option that allows users to connect to Multiple Domains.Auth.Rushfiles components, which enables access to multiple servers from the same client application.

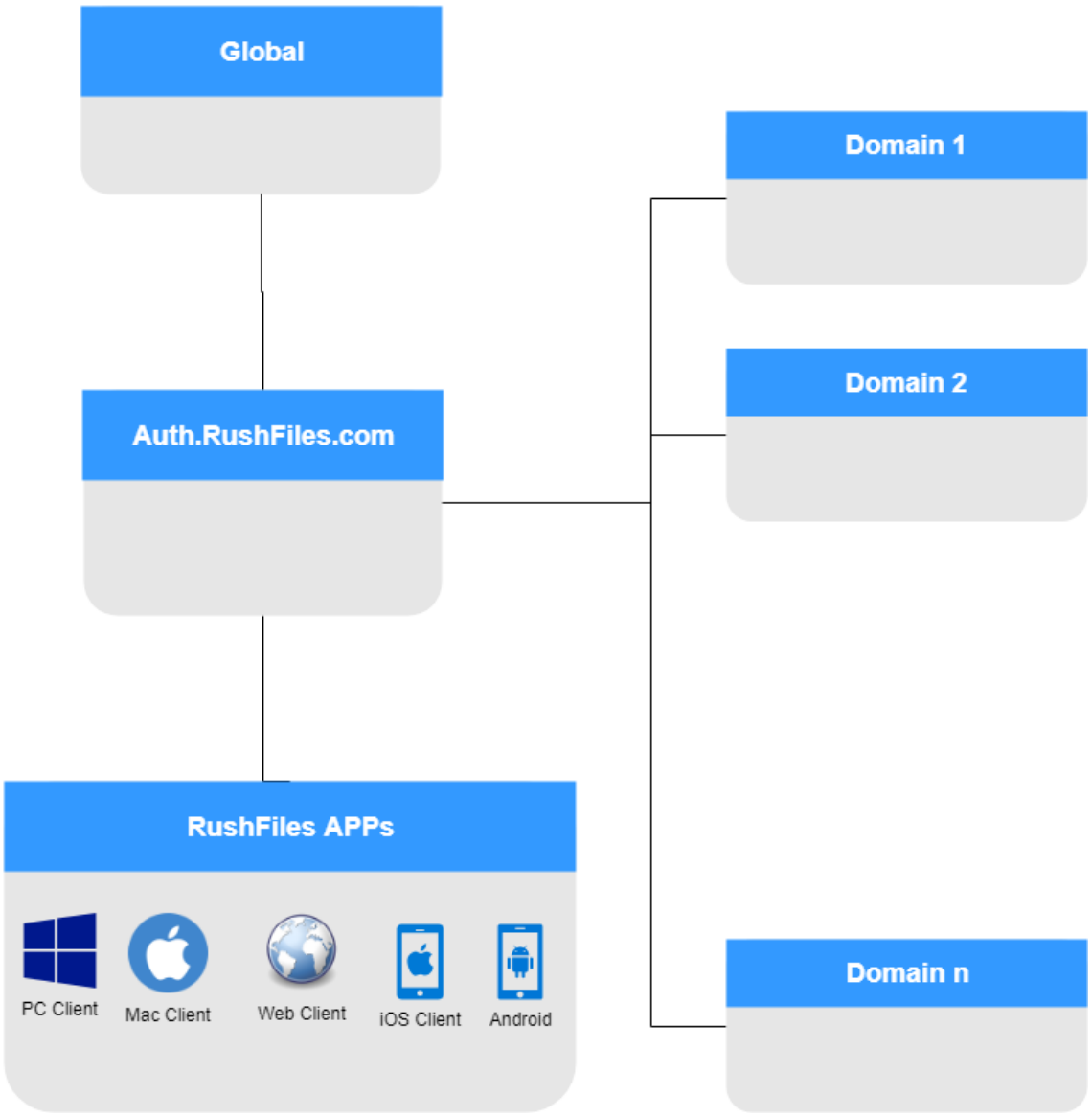

Figure 7- Multiple Domain Login with Auth.RushFIles.com

The login mechanism in this setup will be modified. Instead of interrogating our Global component and returning this information as a client application, Auth.RushFiles component will automatically forward the user, based on the email address, to the primary domain where the user belongs to. After entering the password, the Auth.domain component on the primary domain will validate the user's credentials by providing a token. This token will be 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 for gathering information (see Figure 8).

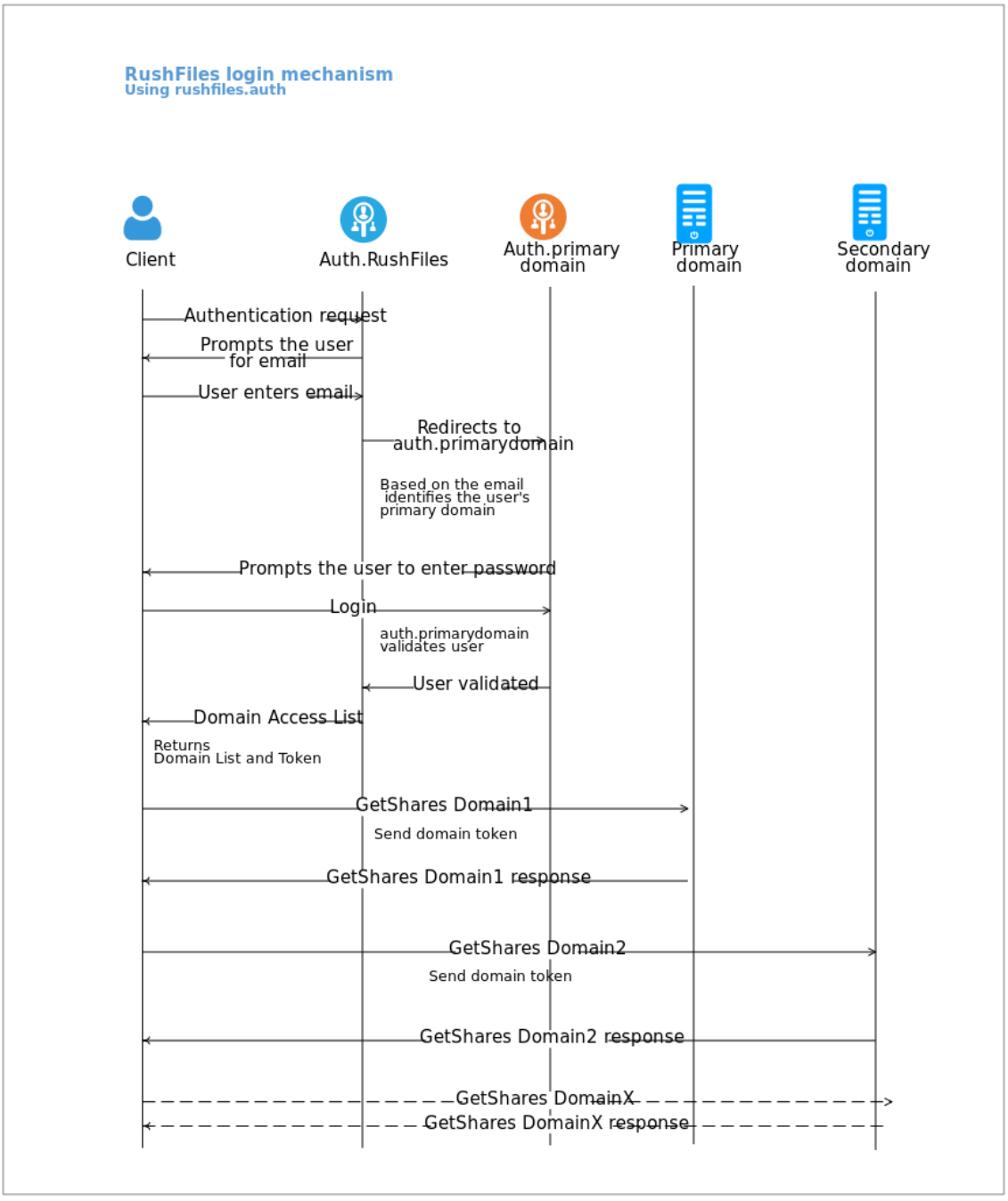

Figure 8- Login mechanism with Auth.RushFiles

2.2.2. Isolated Data Island

In the Isolated Data Island setup, we are introducing the Identity Provider component which will enable SSO for this setup as well. The Domain.Auth will be the primary Identity Provider used for user authentication with the extensibility option through integration with other External Identity Providers (as described in section 2.2.1).

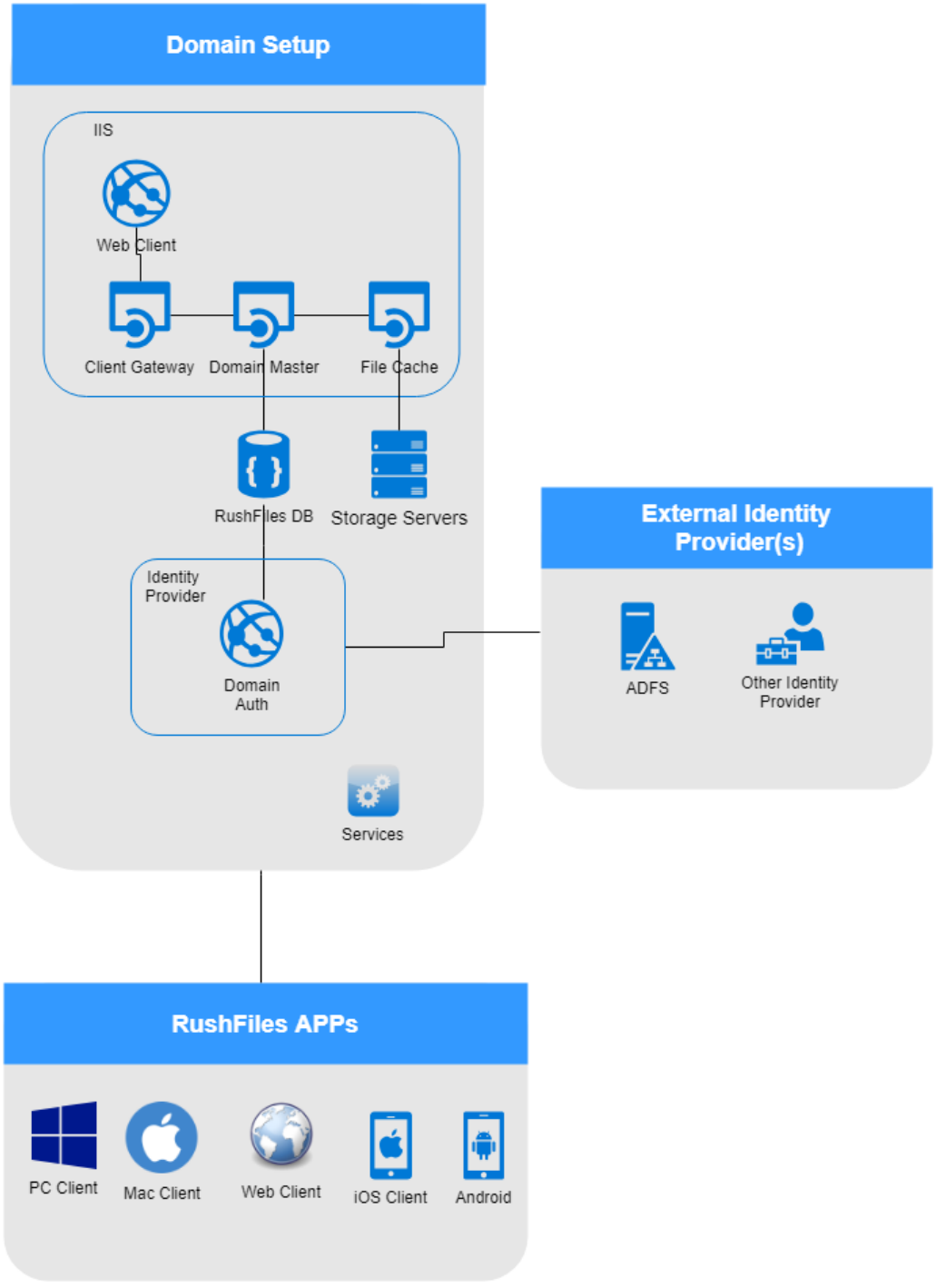

Figure 9- Data Island with Domain.Auth

Like the existing Data Island setup, all communication will be made inside the network, with no interaction with external components.

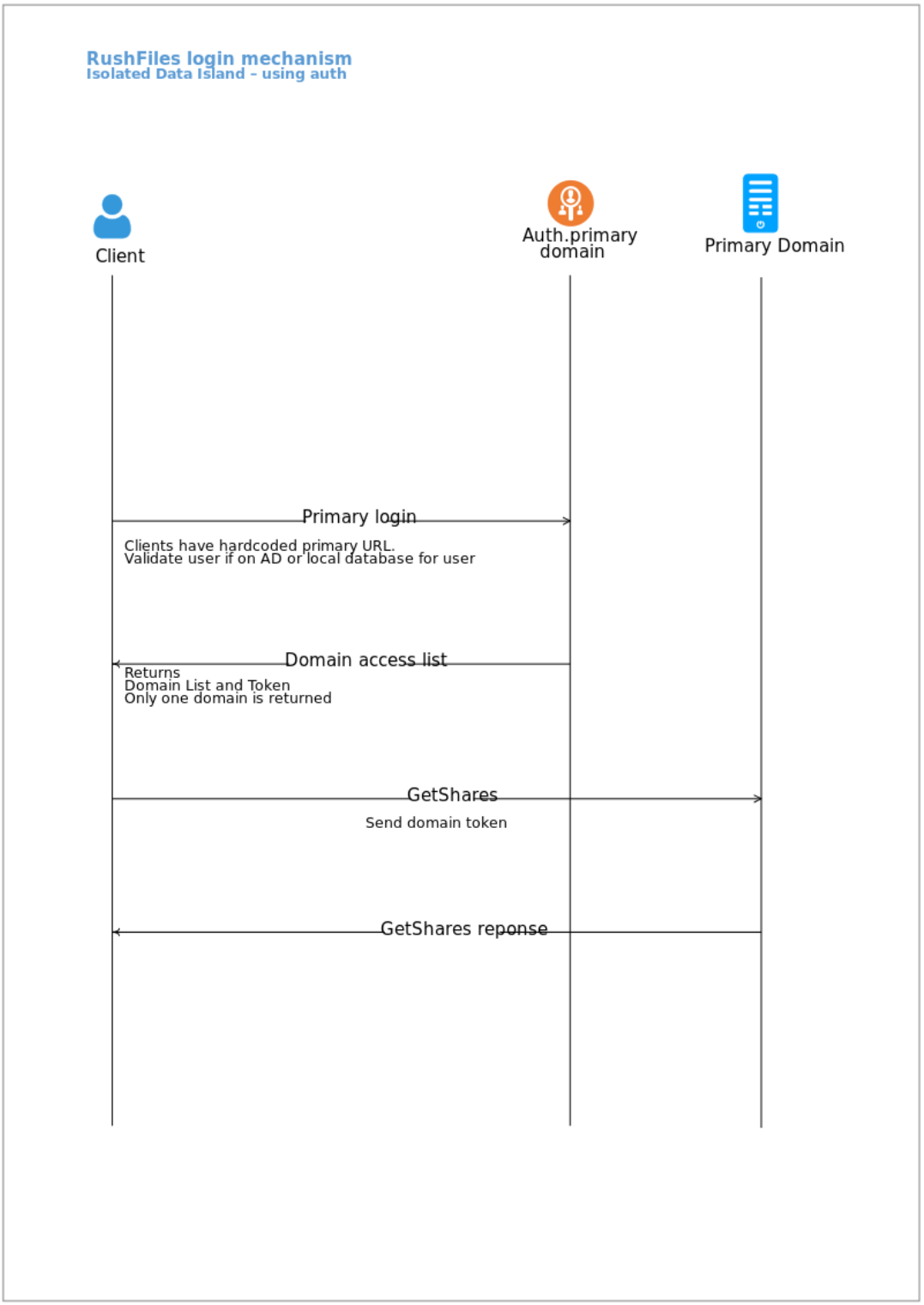

Figure 10- Login Mechanism using Domain.Auth for Data Islands

3. SECURITY

In this section, we will present the current existing security measures implemented by RushFiles, but also the future ones that will be introduced with the Architectural changes that are proposed.

3.1. Current security features

3.1.1. 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. 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 that is running the RushFiles services. Moreover, RushFiles recommend the use of minimum 2048-bit wildcard certificate that is signed by a trusted CA.

3.1.2. File encryption

All files are encrypted on our servers. All files are encrypted using AES (Advanced Encryption Standard) 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.

3.1.3. Obfuscation of data on partners servers

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

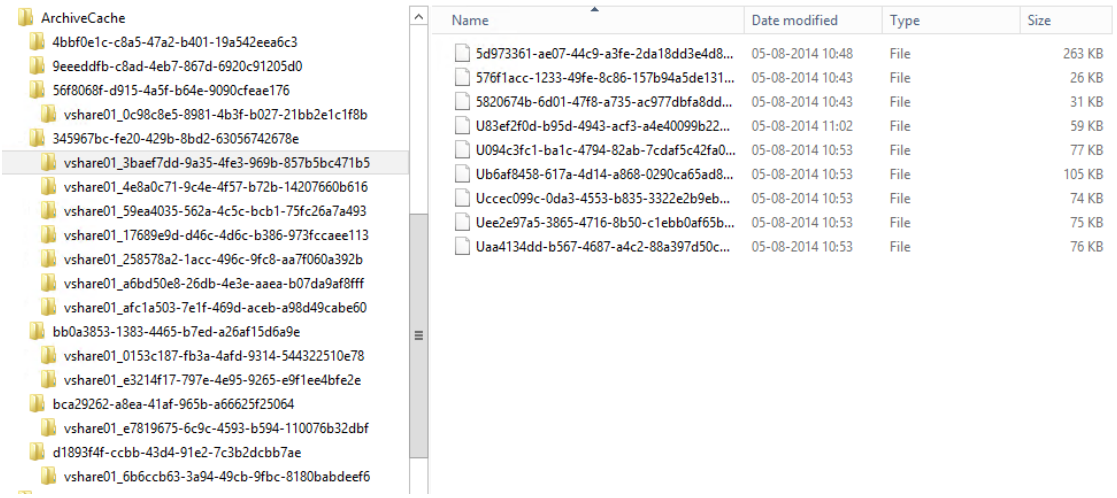

Figure 11 - Example of obfuscated files on the server

The purpose of encryption at the server level would be to prohibit the server administrator from accessing the file content.

3.1.4. Authentication

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

Password security with use of AD integration
For users that are set up to use AD, their password is only stored in the AD. The password rules that apply in the AD is enforced since RushFiles always authenticate the user credentials through Single Sign On (SSO) directly in the AD.

Password security without AD integration
If the organization doesn't have AD integration, the standard RushFiles password security rules apply, and the password must be strong such that it includes:

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

Only the individual user can change the password by requesting a onetime link send to the email address that the user had used to register. Company administrator has an option to resend the reset password email but cannot set the password for their users.

3.1.5. API communication

All communication from client apps to servers is authorized using tokens generated by Domain Master. All APIs validate that the token passed through authorization headers in order to make sure our APIs are not accessed for malicious purposes.

3.1.6. Data islands

Isolated Data Island is a highly restrictive and highly secure version of RushFiles that is offered to our partners. The Isolated Data Island means that the Partner's setup bypasses our Global component that is used to discover domains to connect to, and uses their own installation to access accounts.

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

Data Island requires skinning the client's applications to target your domain URL, meaning users will need a specific white labelled client application to access their data.

3.2. Future security features

3.2.1. Authentication

The authentication of users will be handled on the Primary domain of the user, where Domain.Auth will be acting as an Identity Provider. The user management, including sensitive account information, is ensured by a secure membership system ASP.NET Identity.

The Auth.Rushfiles component will be in charge to redirect the users to the primary domain the user is assigned. Auth.Rushfiles component will store information regarding the list of domains where the user is assigned.

Also, log in using AD and other Identity Providers will be handled on our partners' servers.

3.2.2. Data islands

Like our offered setup, Isolated Data Islands will not use our Global or Auth.RushFiles component to discover domains to connect to it. Users will have access to only one domain setup.

Users will be required to use a specific white labelled client to access user's data.