WHITE PAPER
VERSION 1.0 JUNE 2023

Mediaflux®, A Multi-Factor Authentication, and Authorisation Enabled Data Fabric

Jason Lohrey
Chief Technology Officer

Robert Murphy
VP Product Marketing

Arcitecta Pty. Ltd.

www.arcitecta.com
talk@arcitecta.com

Abstract

In today's digital age, the security of data is of utmost importance. Data repositories and file systems contain large amounts of sensitive information that must be protected from unauthorised access, alteration, or deletion.

Arcitecta Mediaflux provides multi-factor authentication and authorisation (MFA&A) at the very core of the system, including through global file systems of federated storage. Mediaflux MFA&A confirms a person's identity during authentication (when they seek initial access) and for authorisation / approval when attempting to perform sensitive data operations, thus preventing unauthorised access, modification, and deletion, as well as providing enhanced accountability through audit trails.

This paper highlights the benefits of MFA&A, including increased security, reduced risk of data breaches, compliance with industry regulations, and cost-effectiveness.

Introduction

The security of data is a critical aspect of any system use to store and manage data. This is increasingly import and with a rise in the frequency of cyberattacks, as external actors seek to gain advantage from the troves of intellectual property and sensitive data amassed by corporations and institutions. It's not only external actors that pose a threat. There are also threats from insiders /staff attempting to gain illegitimate access. MFA&A can also prevent accidental access or modification of data.

We store information in a variety of systems including a) structured databases, b) asset and data management systems, and c) file systems. Many of these systems contain sensitive information that requires protection from unauthorised access, alteration, or deletion. Most of the systems in use today for managing data do not employ contemporary techniques that enhance the protection of that data, such as multi-factor. Whilst they have been around for decades, the security of file systems has not advanced significantly and their security measures remain weak and insufficient. Mediaflux introduces multi-factor to provide strong security for all data access vectors, including file-system protocols.

The use of second factors (hardware token, phone, and even SMS etc.) has been shown to significantly improve the reliability of establishing a person's identity for the purpose of authentication – that is, when a person connects to a system they are asked to confirm their identity using a) a password – something they know, and b) a security device or token – something they have. That same mechanism can also be used to re-assert a person's identity before they do something with the data such as attempting to access or delete it.

It is worth noting that MFA on a Virtual Private Network (VPN) is not a sufficient level of protection, as a system compromised with malware will not be protected by the VPN. Once the person authenticates via the VPN, and their account has elevated permissions, then a lot of damage can be done. It is interesting observing the reaction of customers when they see that weakness and realise the amount of damage that could be done via administrative accounts in systems with petabytes of data.

In combination, multi-factor authentication and authorisation (MFA&A) are a critical security measure that provides much stronger security, increased control over system access, and reduce the risk of data breaches. They also ensure compliance with industry regulations and are a cost-effective solution for data security. By implementing MFA&A, organisations can protect their sensitive data and ensure the integrity of their file system.

Arcitecta Mediaflux provides multi-factor authentication and authorisation at the core of the system, including the global file system of federated storage systems. Mediaflux MFA&A confirms identity during authentication and is also used when subsequently authorising data operations. For example, deletion may not be allowed unless the person attempting to delete is authorised and acknowledges the deletion using their phone as a second factor. Imagine hard destruction or modification of data requiring a quorum of people to agree to destruction before that can occur in the first place. That is only possible with multi-factor.

Mediaflux multi-factor is available to every protocol including file system protocols such as SMB and NFS, and sFTP along with every other protocol Mediaflux supports including API over HTTP/S, web access, DICOM, etc. The second factor is Mediaflux Pocket – a mobile application for IOS and Android.

MFA&A Benefits

Stronger Security

MFA&A is a highly effective security measure that provides strong protection against unauthorised access to the (file) system. It makes it much more difficult for hackers to gain access to the system as they would need to bypass multiple authentication factors. Multi-factor authorisation requires users to provide at least two forms of authentication. This makes it more difficult for attackers to impersonate legitimate users and gain access to sensitive data.

Preventing Accidental or Unauthorised Deletion

File system multi-factor authentication prevents accidental or unauthorised deletion of files by requiring additional authentication factors before allowing users to delete files. This additional authentication factor ensures that only authorised users with proper clearance can delete files, reducing the risk of accidental or unauthorised deletion. In addition, Mediaflux provides audit trails and activity logs that record who performed what action in the file system, including file deletions.

These logs are used to monitor and track changes to the file system, providing an additional layer of forensic analysis and accountability.

Increased Control

MFA&A provides increased control over who has access to the file system. System administrators can customise the authentication and authorisation process to ensure that only authorised users can access the system. This prevents unauthorised access to sensitive data and protects the integrity of the file system.

The policy for MFA&A can be set per file, per collection/directory and/or system wide. It can also be set as a function of the roles a person holds.

Reduced Risk of Data Breaches

MFA&A reduces the risk of data breaches by making it more difficult for hackers to access the system. Even if a hacker manages to obtain a user's password, they will still need to provide additional authentication factors to gain access to the system.

Audit Trails

Multi-factor authorisation enhances the accuracy and completeness of an audit trail by providing more detailed information about user activity, including authentication and authorisation factors.

Multi-factor authorisation provides an additional layer of authentication and authorisation that is recorded in the audit log. Multi-factor authorisation provides more granular details about who accessed a system, when, and for what purpose. For example, if a user attempted to access a system with multi-factor authorisation, but was unable to provide the additional authorisation factor, this information would be logged in the audit trail. Similarly, if a user attempted to perform a sensitive action such as deleting a file but was required to provide additional authorisation factors before completing the action, this would also be recorded in the audit trail.

The audit trail is used to identify and investigate security incidents or suspicious activity, as well as to monitor compliance with organisational policies and regulations. By providing more detailed information about user activity, multi-factor authorisation ensures the integrity and accuracy of the audit trail, which is critical for forensic analysis and legal compliance.

Compliance with Industry Regulations

Many industries, such as healthcare and finance, have strict regulations that require the use of MFA&A for data security. Implementing MFA for a file system ensures compliance with these regulations and protects sensitive data.

Cost-Effectiveness

While the implementation of MF&A may require additional Mediaflux hardware and software, it is a comparatively cost-effective solution for data security. The cost of a data breach is much higher than the cost of implementing MFA&A.

Aiding Forensic Investigations

Multi-factor can be helpful in forensics investigations by providing additional layers of authentication and authorisation that can be used to trace and verify user actions in the system.

Here are some ways in which multi-factor authorisation can help with forensics:

Verification of User Identity

Multi-factor can help to verify the identity of users accessing the system, as it requires users to provide multiple factors of authentication or authorisation. This can help to prevent unauthorised access and ensure that actions performed in the system are associated with a specific user identity, which can be critical for forensic investigations.

Granular Details About User Actions

Multi-factor can provide more detailed information about the specific actions performed by users in the system. For example, if a user attempts to perform a sensitive action such as deleting a file, a multi-factor may require additional authorisation factors such as approval from a manager or a confirmation message. This information can be critical in forensics investigations, as it can provide more granular details about the user's intent and motivations.

Preventing Data Theft

Multi-factor authorisation can help protect against data theft by providing an additional layer of security beyond just a username and password. Here are some ways in which multi-factor authorisation can help protect against data theft:

Protection Against Phishing Attacks

Multi-factor authorisation can also help protect against phishing attacks, where attackers attempt to trick users into revealing their login credentials. Even if an attacker obtains a user's password through a phishing attack, they will still need the second factor of authentication to gain access to the system.

Access Control

Multi-factor authorisation can also help to enforce access control policies, such as restricting access to sensitive data based on user roles and permissions. This can help to prevent unauthorised users from accessing sensitive data, even if they have obtained valid login credentials.

Monitoring and Alerts

Multi-factor authorisation can also provide additional monitoring and alerting capabilities, such as sending notifications when a user logs in from a new device or location. This can help to identify suspicious activity and alert administrators to potential security threats.

Mediaflux Workflow Authentication and Authorisation

With Mediaflux, every user or system is identified and authenticated to ensure that they can only access, create, modify, and delete assets that they are authorised to see or modify. Mediaflux supports several authentication systems (individually or in combination), including LDAP, Active Directory, Kerberos, SAML, and Local. The authentication is modular and can be extended, and it can be configured to be specific to a single system or recognised throughout a federation of servers.

Mediaflux authentication and access can be restricted to specific IP address ranges and restricted to people with specific roles. The server includes protection against brute-force password attacks for local accounts and can enforce high-strength passwords through configuration.

MFA&A can be enabled per user domain or for specific users. Anything in the system can be protected with MFA&A such as services, directories and files or fragments of metadata.

Once authenticated, a user can only perform functions they are permitted to, including access to specific services, sets of data, and fragments of metadata. Authority can be organised into hierarchical groups or roles, and users can be assigned roles that embody the requisite level of permissions.

In addition to role-based access controls (RBAC), attribute-based access controls can specify special conditions of access. For example, "only people with brown eyes and not taller than 180cm can access file F, provided that it's the first Wednesday of the month". The expression of attribute based security can be arbitrarily complex.

Mediaflux only shows metadata and data to which the user has access and will never indicate the existence of an object if the user does not have the authority to access it. It is possible to allow access to the metadata but not the actual data itself, which allows the caller to discover the data but may require completing another process to gain access to it. Mediaflux audits every operation, and the auditing can be configured to record selected operations, including changes or requests to access every element of data. Auditing is not a primary defence but is important for both security review and reporting on data usage and access patterns.

MFA&A and the File System

Mediaflux presents data concurrently through file-system protocols such as SMB and NFS, along with the S3 object protocol, and a raft of other protocols. Access via a file system may trigger MFA&A. For example, when a user authenticates to an SMB share, they may be required to assert their identity using MFA. Protocols such as NFSv3 have relatively weak identification using client provided UID which is mapped to a user. The security of these weaker forms of protocol can be vastly improved with MFA. For example, access to an NFS share with a UID can trigger a request to confirm a person's identity via MFA. This need not happen for every access – the frequency of revalidation can be configured.

When I decide to delete a file, then Mediaflux multi-factor authorisation will confirm it's me. Perhaps that's only required for some files and not others – that's a matter of policy and configuration. I assert it's me and the delete proceeds. Due to a deletion policy, the deletion is soft. For a file to be hard destroyed, the deletion policy might require 3 out of 5 people to confirm the destruction should take place – they need to confirm their approval through MFA&A.

You might think that this could become onerous on a general file system. However, the level of verification is controlled by policies, and a policy might require the modification or deletion of every file to be validated through MFA&A, or it might be restricted to certain sensitive files or files that are expensive to regenerate. The level of granularity is up to every data owner / custodian – it can be as broad or granular as you like. If permitted, you can batch-approve larger requests to reduce the number of approvals required.

Industries That Benefit from MFA&A

Multi-factor authentication and authorisation (MFA&A) can benefit a wide range of industries that handle sensitive data, including but not limited to:

Research

Research organisations handle sensitive data related to intellectual property, medical research, and scientific discoveries. MFA&A protects this information from unauthorised access and ensures the integrity of the research.

Healthcare

Medical records contain sensitive and confidential information that needs to be safeguarded from unauthorised access. MFA&A makes sure that only authorised personnel can access this information.

Finance

Financial institutions deal with sensitive financial information, such as bank account numbers and social security numbers. MFA&A defends against data breaches and ensures compliance with industry regulations.

Government

Government agencies handle sensitive data such as national security information, law enforcement records, and personal identification information. MFA&A provides an additional layer of security to protect against unauthorised access and data breaches.

Legal

Law firms and legal departments handle confidential information related to legal cases and client information. MFA&A protects against unauthorised access to this information and ensures the integrity of the legal system.

Education

Educational institutions handle sensitive data such as student records, financial aid information, and research data. MFA&A ensures that this information is safeguarded from unauthorised access and data breaches.

Defence

Defence organisations handle sensitive national security information, military strategy, and classified documents. MFA&A provides an additional layer of security to protect against unauthorised access and data breaches.

Manufacturing

Manufacturing companies may handle confidential information related to product design, manufacturing processes, and supply chain management. MFA&A shields this information from unauthorised access and data breaches.

Summary

Multi-factor authentication and authorisation (MFA&A) are critical security measures that provide stronger security, increased control over system access, and reduced risk of data breaches.

Arcitecta Mediaflux provides MFA&A across a global file system of federated storage systems, providing organisations with increased control over who has access to the file system and protecting sensitive data. The benefits of MFA&A include stronger security, prevention of accidental or unauthorised deletion, increased control, reduced risk of data breaches, compliance with industry regulations, and cost-effectiveness. Additionally, MFA&A provides granular details about user actions, which is critical for forensic analysis and legal compliance. Implementing MFA&A ensures the integrity and accuracy of the audit trail, which is crucial for identifying and investigating security incidents and suspicious activity.

In the end, it seems obvious to introduce MFA&A to the core of a data management system, which is why we did it. It's easy when you have the right software platform.