INTRODUCTION TO THE NUMEROUS SIGNIFICANT NEW SECURITY FEATURES IN FILEMAKER PLATFORM VERSION 16

By:

Wim Decorte

—and—

Steven H. Blackwell

VERSION 1.0

CONTENTS

Introduction To The Numerous Significant New Security Features In FileMaker Platform Version 16

By:

Wim Decorte
—and—
Steven H. Blackwell

The release of Version 16 of the FileMaker Platform brings with it a host of new security features reaching across the entire FileMaker Platform, from FileMaker® Server 16 to FileMaker® Pro 16 to WebDirect™ and beyond.

In this White Paper we will examine these new features in some detail. One topic in particular, that of the new Federated Identity Management options, will also be covered in much more detail in a second White Paper, although we will introduce it here. This paper consists of five separate sections:

- A brief history of major security improvements in the Platform since the introduction in March 2004 of FileMaker® Pro 7.
- A discussion of some remaining vulnerabilities that required addressing.
- A discussion of how the new versions of the products address those vulnerabilities.
- A discussion of the new Field Level Encryption functionality.
- An introduction to the expansion of Identity and Access Management options resulting from the adoption of OAuth2 functionality.

—Executive Summary and Overview—

The newest version of the FileMaker Platform brings with it additional and much needed security enhancements in two major areas: ***Identity and Access Management*** (I&AM) and ***Privileges Control***. I&AM has been significantly broadened by the addition of OAuth2 based controls to permit Amazon Accounts, Google Accounts, and Microsoft Azure Active Directory Accounts to authenticate users of FileMaker Pro files hosted by FileMaker Server.

In the area of Privileges Control, the new version offers much expanded levels of fine-grain controls over the behavior of three External APIs: ***AppleEvents*** (Macintosh OS), ***ActiveX*** (Windows OS), and ***FMPURL*** script triggering (both platforms).

Identity and Access Management enhancements are important. We will address the in-depth particulars of the new Version 16 I&AM features in a second White Paper.

However, in this paper, we want to note the importance of robust I&AM. When Attackers or Threat Agents view organizational data and IT infrastructure they generally have four main goals[1] in mind:

- To compromise identities
- To impersonate legitimate users to glide past security controls
- To find valuable data
- To glide back out undetected.

FileMaker Platform developers, FileMaker Server Administrators, and the IT professionals who support them need to defeat these four Attacker objectives by having five distinct goals:

- Assure integrity of identities
- Detect intrusions
- Expel intruders
- Preserve Confidentiality, Integrity, Availability, and Resilience of data
- Protect the organization and assure its continuing operation.[2]

Identity is the New Security. Version 16 of the FileMaker Platform takes Federated Identity Management to a new level by employing OAuth2 standards to permit Amazon, Google, and Azure Active Directory to serve as Identity Authentication Services for the FileMaker Platform. In addition to enlarging the I&AM horizon, this expansion facilitates the rapid provisioning of new FileMaker Platform systems to multiple users in multiple locales with greater ease and fewer errors.

BRIEF HISTORY OF SECURITY FEATURES IN THE FILEMAKER PLATFORM

The advent, on March 10th 2004, of the modern-era FileMaker Platform with FileMaker® Pro 7 brought with it an entirely new approach to security,[3] both I&AM and Role Based Privileges. Proper Account Names, passwords, and data and UI privileges defined through Privilege Sets became the norm for the Platform. This was a dramatic

[1] RSA. *A New Paradigm For Identity Assurance*. (2016, Santa Clara, CA. www.rsa.com)

[2] http://fmforums.com/blogs/entry/1523-aligning-filemaker-security-requirements-to-business-interests/

[3] Blackwell, Steven H. *Upgrading To FileMaker 7: How To Employ The New, Advanced Security System*. (FileMaker, Inc. Santa Clara, CA. 2004) http://fmforums.com/files/file/87-security-tech-brief-1-fmp-7/ and *Using FileMaker Pro 9. How to Employ the New, Advanced Security System*. (FileMaker, Inc. Santa Clara, CA. 2007) http://fmforums.com/files/file/88-security-tech-brief-2-fmp-9/

change from earlier versions. These new features placed the Platform squarely inside the envelope of Information Industry standards and practices.

Two additional highly significant aspects of FileMaker Platform security also appeared with the release of FileMaker® Server 7. One of these was *Encryption In Transit* that protects data from prying eyes as the data travel over networks. The other, also a feature of FileMaker Server 7, was *External Server Authentication*, whereby Open Directory, Active Directory, and Local Security Group Accounts and Groups could be used in conjunction with FileMaker Server hosted files for I&AM purposes.[4]

With minor refinements and adjustments, notably to External Server Authentication, the Platform then remained static regarding security features and enhancements until the release of Version 11 of the FileMaker Platform in March of 2010. FileMaker® Pro 11 introduced an ***exceptionally significant*** security feature: *File Access Protection*.[5] At its base, this feature prevents unauthorized use of external rogue FileMaker Platform files to "peer into" other FileMaker Pro files and to extract information or to perform actions such as running of scripts, *all in a manner unintended by the developer, and usually unknown to the developer.* **It is difficult to over-emphasize the significance of this security feature and its usefulness in protecting systems.**

The next major security enhancement came with the introduction of FileMaker® Pro 13 in December of 2013. *Encryption At Rest* protects the physical FileMaker Pro binary file from unauthorized access.[6] Given the ubiquity of password crackers, binary extraction tools, and similar devices, this is an important protection. Additionally, lost or stolen backup copies of database files are a major attack surface for Threat Agents. Encryption At Rest (EAR) helps protect files from all these vulnerabilities.

Version 14 of the FileMaker Platform, released in May of 2015, brought two significant additions to the security schema. The *FileMaker Server Sample File*, something that had been around since at least Version 7, had several significant security vulnerabilities that could enable it to serve as an attack vector for all hosted files on a server.[7] Version 14 closed those by removing the [Full Access] Privilege Set from the file.

Another issue was that in many instances users would store their credentials in the *KeyChain* (Macintosh OS) or in the *Credentials Manager* (Windows OS). This often produced undesirable results, unexpected results, or both. FileMaker® Pro 14 provided

---

[4] Decorte, Wim and Blackwell, Steven H. *Server External Authentication*. (FileMaker, Inc. Santa Clara, CA. 2007) http://fmforums.com/files/file/89-external-server-authentication/

[5] http://www.fmpug.com/resources/security_schema_changes_filemaker_11

[6] http://fmforums.com/blogs/entry/709-newest-version-of-filemaker-platform-brings-significant-major-security-enhancement/

[7] http://fmforums.com/blogs/entry/777-protect-your-filemaker-server-and-files-from-a-vulnerability/

an option for developers to block storage of such credentials. Moreover, if a user had stored credentials, invoking this new option would render the FileMaker Pro file impervious to use of those credentials.[8]

Version 15 of the FileMaker Platform, introduced in May of 2016, brought two additional important security enhancements.[9] One of the reasons that the previously mentioned FileMaker Server Sample File constituted a rich attack vector was that it would open to [Full Access] without any credentials challenge, either by the auto-open feature or by default credentials. Unfortunately many FileMaker Server deployments not only suffered from this vulnerability but also from a concomitant one. Developers would also include such unprotected files on FileMaker Server installations. FileMaker® Server 15, *by default, will not host insecure files*. Such files are defined to be these:

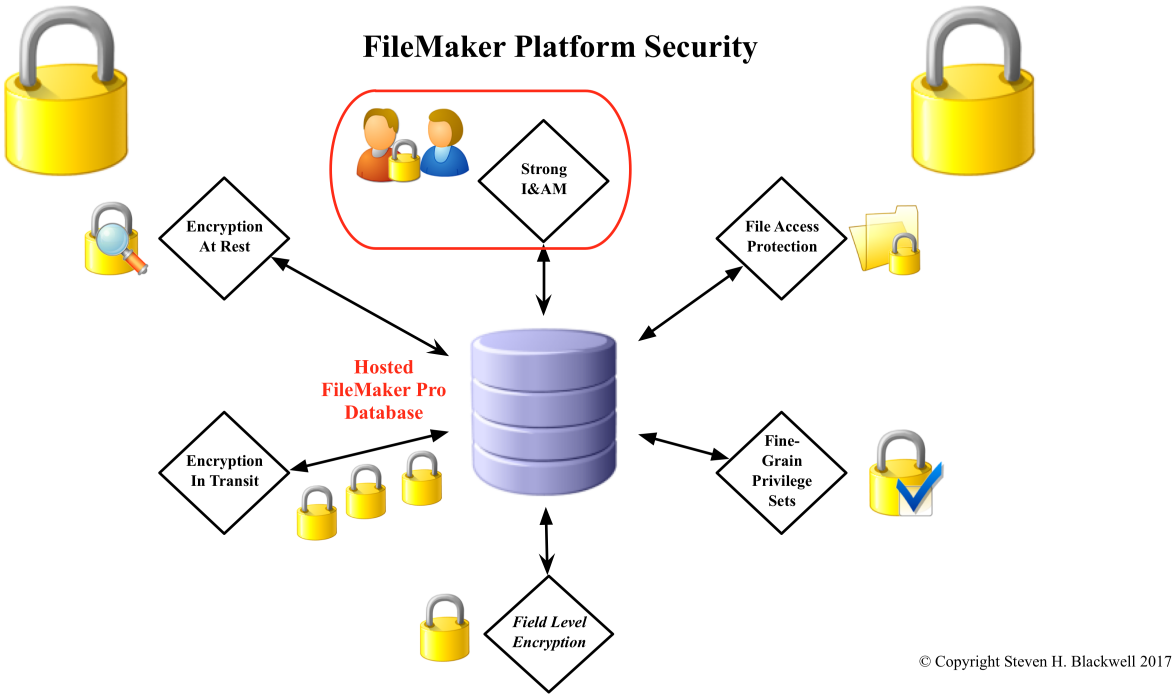
- Guest Account enabled and attached to the [Full Access] Privilege Set
- A [Full Access] Account with no password
- A [Full Access] Account with the password stored using the File Options "Log In Using" feature.

In addition to blocking insecure hosting, FileMaker® Pro 15 Advanced brought with it another feature. The *Data Viewer* is an advanced developer functionality that is useful for any number of tasks. The Viewer has two different tabs: *Current* and *Watch*. Access to the *Current* tab requires [Full Access] credentials either to have opened the file or to be entered by clicking a lock icon in the *Current* tab window. However, prior to Version 15, subordinate level Accounts could open and use the processes in the *Watch* Tab. While there were restrictions a Privilege Set could impose on the breadth of the actions a user with a subordinate Account could undertake, there nevertheless was a vulnerability here. So, in FileMaker Pro 15 Advanced, access to the Watch Tab also requires [Full Access] authentication.

So, when we approach the FileMaker Platform today we see an entire range of features in the Security Schema all focused on strong Identity and Access Management and on management of Role-Based Privileges. The diagram below presents that information in a consolidated and unified format. All that said, there are still items left to consider to provide optimal security to FileMaker Platform files in a variety of circumstances.

[8] http://fmforums.com/blogs/entry/1369-filemaker-14-platform-brings-new-security-features/

[9] http://fmforums.com/blogs/entry/1541-new-security-features-in-version-15-filemaker-platform/



FileMaker Platform Security Schema Elements Diagram

—SOME REMAINING VULNERABILITIES—

The dozen years of the modern FileMaker Platform era, running from March 2004 to May 2016, saw all these improvements and enhancements to FileMaker Platform security features. However, considerable vulnerabilities remained in the products that needed addressing. Most of these focused on the behavior of **External Application Programming Interfaces (APIs).** These vulnerabilities were significant; and, for the most part, most FileMaker developers, including highly experienced ones, had little awareness of them or of their potentially serious impact. **What are these vulnerabilities?**

- There are significant issues related to the *Data Layer* of a FileMaker Pro file. APIs could perform a variety of actions on files that could lead to their compromise:
  - They could extract data from one record or from many records.
  - They could extract metadata from a file, including Script Names, Layout Names, Value List Names, and Value List Items.
  - They could set data into fields in one or more records.
  - They could create[10] and delete records in a table.

[10] This was a favorite method of defeating record creation restrictions in so-called demo versions of FileMaker Pro files.

- Likewise, there are significant issues related to *Scripts and Business Logic Layer* in FileMaker Pro files:
  - External APIs could trigger scripts, including providing optional parameters.
- There are issues related to the *User Interface*:
  - External APIs could manipulate the User Interface of files.
  - Such manipulation could traverse to so-called "hidden" layouts, exposing their contents.[11]

Developers could control many of these elements to some degree through careful security design and business logic construction. But there were still vulnerabilities that even carefully designed Privilege Sets did not control. **And, as we have previously noted, many developers were simply unaware these vulnerabilities even existed, much less know how to control them.**

So, what was needed? Clearly we needed to strengthen the security posture of the FileMaker Platform and to give developers affirmative controls over the behaviors of these APIs. **The Threat Agent (Attacker) does not care if the developer understands the behavior of these APIs. The Threat Agent sees them as vulnerabilities to be exploited to facilitate an attack on the database system.** And, in the end, it is the **Strength of the Defender, not the Strength of the Attacker**, that determines the outcome of the attack. And developers need all the strength we can muster.

So, in Version 16 of the FileMaker Platform, FileMaker, Inc. has provided a series of new tools to help address these vulnerabilities.

—How The New Version Addresses These Vulnerabilities—

As noted, several External APIs can provide unexpected attack vectors for manipulating and compromising FileMaker Pro files. These APIs specifically include the following:

- **AppleEvents** on the Macintosh OS platform
- **ActiveX** on the Windows Platform
- **FMPURL** functionality on both platforms

These attacks can have significant impact on the database files. And they can compromise the Confidentiality, Integrity, Availability, and Resilience of files, as detailed at length in various articles and BLOG posts:

---

[11] And if developers carelessly left significant information such as credentials (and yes that has happened), flag fields designed to enforce restrictions, and similar elements exposed on the layout, then they could be used or manipulated.

a. http://fmforums.com/blogs/entry/1535-the-filemaker-platform-api's-are-your-friends-right/
b. http://fmforums.com/blogs/entry/1652-security-vulnerabilities-of-filemaker-platform-api's-an-update/
c. http://fmforums.com/blogs/entry/1411-some-vulnerabilities-associated-with-ersatz-log-on-systems/
d. http://fmforums.com/blogs/entry/1512-a-conversation-about-2-factor-authentication/ [12]

So, we needed an enhanced ability to control these actions. FileMaker® Pro 15 began efforts to control some of the External API behavior with the addition of the *fmscriptdisabled* functionality. That feature was a Privilege Bit in the Extended Privileges section of a FileMaker Pro Privilege Set, as shown here in Figure 1.

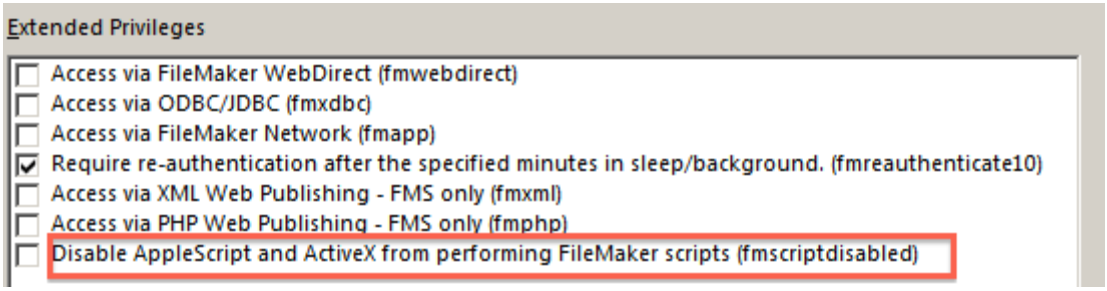


Figure 1. The fmscriptdisabled Privilege Bit, FileMaker Pro 15.

This functionality's purpose was to block AppleEvents and ActiveX from triggering scripts in FileMaker Pro files. It was a good start; however, there were a number of issues with this approach:

- First, developers had to enable it affirmatively in order for it to work. The *default behavior was to allow* the APIs to run the scripts.
- Second, this controlled *scripts only*. It *did not control other actions* that the APIs (particularly AppleEvents) could take.
- Third, it did not control the FMPURL APIs capability to trigger scripts.

—New and More Comprehensive Approach—

FileMaker Pro 16 takes a new and much more comprehensive approach to controlling these APIs and their behaviors. **By default**, these APIs **do not run** to perform

[12] Courtesy Joshua Ormond, *Eye on FileMaker* BLOG http://fmforums.com/blogs/entry/1512-a-conversation-about-2-factor-authentication/

actions in the files. This is consistent with the ***Rule of Least Privileges***[13] and enforces the requirement that any given privilege must be explicitly enabled. Otherwise, the Privilege Bit is *Off*.

As shown in Figure 2 below, the new process requires developers ***specifically*** and ***affirmatively*** to select an option in a given Privilege Set: ***Allow AppleEvents and ActiveX to perform FileMaker operations…***

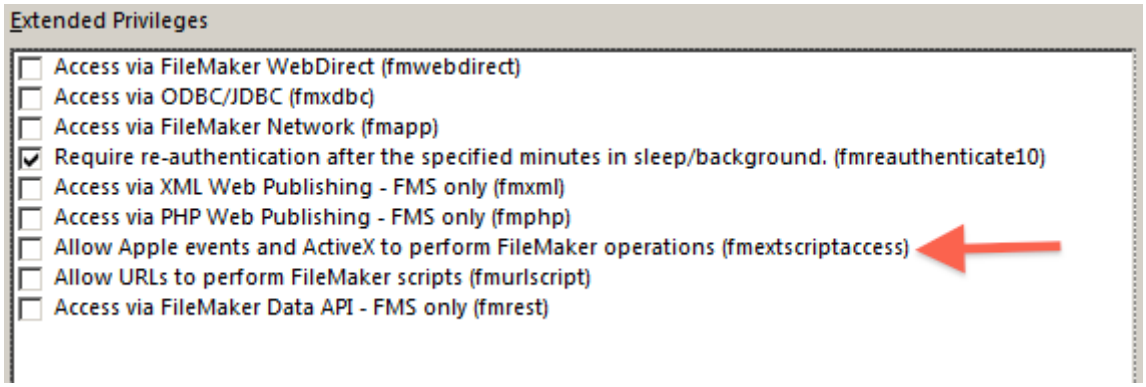


Figure 2. Allow AppleEvents and ActiveX to perform FileMaker operations…

This Privilege Bit controls four actions in AppleEvents and one action in the more limited ActiveX API.

- Script triggering by AppleEvents
- Metadata extraction by AppleEvents
- Data extraction and insertion by AppleEvents
- User Interface manipulation by AppleEvents
- Script triggering by ActiveX

Take a second look at this same screen as shown below in Figure 3. Note that there is another Privilege Bit: ***Allow URLs to perform FileMaker scripts.*** As is the case with its companion privilege, developers must ***explicitly enable*** this in order to use the FMPURL process to trigger a script in a FileMaker Pro file.

Using the process described in considerable detail in FileMaker Tech Info 5560 (http://thefmkb.com/5560), developers can trigger a script in a file using this format:

fmp://0.0.0.0/database.fmp12?script=scriptname

where the IP address of the server replaces the 0.0.0.0 construct, and where the actual script name replaces the *scriptname* placeholder.

[13] That rule basically holds that users in a specific Role should have all the privileges needed to fulfill the responsibilities of the role, but that they should have no additional nor higher-level privileges. ***We work to prevent unauthorized escalation of these Privileges.***

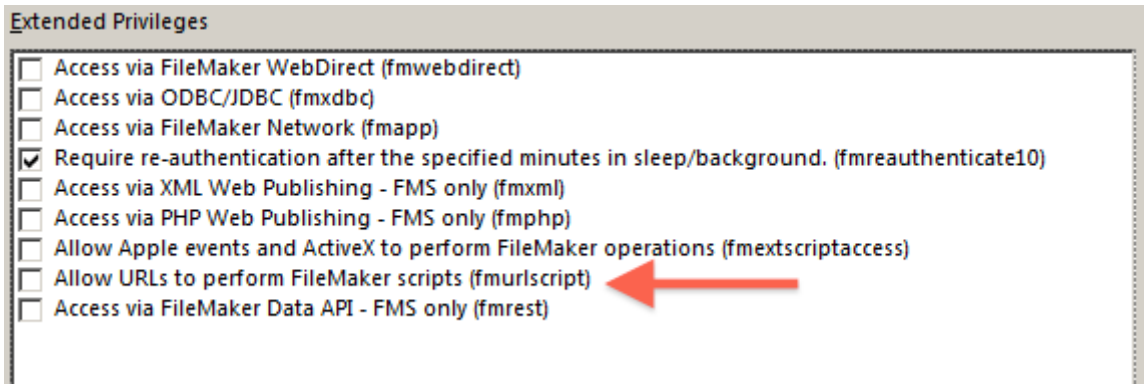


Figure 3. Allow URLs to perform FileMaker scripts…

Starting in Version 16, the Privilege Bit as shown must be *active* in order for the script to run. By default the Privilege Bit is now *inactive*.

—A Better and More Secure Process—

This entire process with all three of these APIs is much more secure than was the case in the past. There are several reasons for that and several considerations for developers going forward:

- ❖ Please note again that these APIs now require *explicit enablement* in order for them to work.
- ❖ This means that unless the Privilege Bit is enabled that the API **will not interact** with the file.
- ❖ When files that started in earlier versions are used with Version 16, developers must reset Privilege Bits in those files if the API is to work.

The security schema now works by **default** to **prevent** AppleEvents and ActiveX from sending commands to these files. In the instance of AppleEvents, this also pertains to the internal *Perform AppleScript* script step.

- Developers can enable the capabilities of AppleEvents and ActiveX by activating the Privilege Bit on a Privilege Set by Privilege Set basis. This provides excellent fine-level granularity of control for various Roles in the system.
- This change addresses questions of script manipulations, setting and extracting of data, extraction of metadata, and UI manipulation.

The security schema now also works by **default** to **prevent** FMPURL from triggering scripts in a file. As is the case with AppleEvents and ActiveX developers can enable the ability of FMPURL to call the script by explicitly enabling the Privilege Bit. This avoids having to rely on the *only partially effective* workaround from prior versions of using a *Halt Script* step at the end of any *OnOpen* script in an attempt to control the behavior of FMPURL.

There are some important caveats related to duplicating results of these type attacks by use of other vulnerabilities. Developers must consider all of these as part of security planning.

- ***User Interface manipulation*** can still occur in the file unless access is blocked by File Access Protection.
- ***Metadata extraction*** can still occur in the file unless access is blocked by File Access Protection.
- ***Script manipulation*** can still occur in the file unless access is blocked by File Access Protection.
- ***Opening the file in older versions*** of FileMaker Pro will bypass these new FileMaker Platform Version 16 security features.

—NEW ENCRYPTION FUNCTIONALITY—

Version 16 of the FileMaker Platform introduces several new functions whose purpose is to provide encryption to individual fields in a FileMaker Pro database. **FileMaker developers should take particular care when using these functions and be sure that they understand how they work, what they do, and what they do not do.**

A few important caveats:

- Strictly speaking, these functions *do not operate at the field level.* They operate at the *cell level*, that being the intersection of a field and a record. There may some exceptions to this definition, mainly focused around auto-enter calculations and Record-Level Access calculations.
- ***These functions are not part of the I&AM portion of the security schema.*** They are not for use in Identity and Access Management construction. This is a significant consideration. Misuse of these functions will likely lessen the security of a file as we have seen in countless incidents over the years.

The basic principle underlying the use of the new encryption functions is rather straightforward. Give some field named, for example, ***SecretField***, this is one syntax to encrypt that field:

CryptEncrypt (*SecretField*; *key*)

FileMaker, Inc. notes: [14]

> The value in the parameter *key* is any text expression or field to be used to encrypt the data. CryptEncrypt accepts text or container data and returns *container data* as a binary file…. This function uses the PBKDF2[15] algorithm to

[14] Courtesy FileMaker, Inc. (2017, Santa Clara, CA.)

[15] https://tools.ietf.org/html/rfc2898

> convert the key parameter into a cryptographic key. This key is used to encrypt data…. The returned file includes an encrypted SHA256 digest of data, which is used to validate the data during decryption.

Going back the other way, developers would use this functionality to decrypt the container and return the original data:

CryptDecrypt (*container*; *key*)

The parameter *container* refers to the encrypted object; the parameter *key* is the original value used to encrypt the information.

With the advent of the new encryption functions functionality, developers will now need to consider and to address elements of Key Management:

- Key Creation
- Key Storage
- Key Retention
- Key Destruction

In some instances **if a key is destroyed, it effectively destroys the data in the encrypted cell. Without the initial key used to encrypt the data, they remain encrypted and cannot be decrypted.**

Best Practices for Key Creation (Key Generation) certainly will include three essential elements:

- Length
- Complexity
- Entropy

Noted security analyst Bruce Schneier has described a critical item about key length in one of his Crypto-Gram BLOG posts:

> Despite what everyone else tries to tell you, cryptographic key length has almost nothing to do with security. A short key means bad security, but a long key does not mean good security.[16]

We encourage readers of this White Paper to review Schneier's discussion of this item and about what constitutes strong keys.

What are some likely uses for the new encryption functionality? The most immediately obvious one is to protect the confidentiality of data in a field. That is its most likely use as well. Such encryption **does not however replace Encryption at Rest** (EAR). EAR is ***file-level*** encryption and is designed to protect the entire file, including backups, from tampering.

There are other considerations about the use of the new encryption functionality developers should consider before employing it:

---

[16] http://www.schneier.com/crypto-gram-9910.html#KeyLengthandSecurity

- What is the impact or the result of attempting to decrypt data in a cell that is already in plain text, that is to say, already decrypted? The answer is that the Decrypt function can destroy the data in the cell.
- When the contents of a cell are encrypted, subsequently decrypted, and then encrypted for a second time, the **encrypted values will not be same** from the first to the second time, nor from any subsequent time. **This the desired and correct process.** If a developer is relying on the values' being identical, then the process will fail.
- If a key becomes compromised—and that does happen—how does the developer locate all the records with encrypted cells so that these may be decrypted with the compromised key and then re-encrypted with a new key?
- What is the result of encrypting an already encrypted cell? How can such a cell be decrypted?

There is going to be a considerable amount of work that needs to be done in the community in the real world of deployed systems before we can assemble a comprehensive list of Best Practices for these new encryption functions. Until then, indeed even after then, developers should employ caution in this area.

—INTRODUCTION TO FEDERATED IDENTITY MANAGEMENT—

Version 16 of the FileMaker Platform marks the arrival of full-fledged Federated Identity Management. *What is this? Why is it useful or desirable for FileMaker developers? How does it work?*

In a separate White Paper[17] we will cover in extensive detail the configuration and management of Federated Identity Management using the OAuth2 standard that FileMaker, Inc. has adopted. This is both a client-side and a server-side process. But in this concluding section of this White Paper, we will present an introduction to the concept and a brief explanation of how it works.

It could be argued that Federated Identity Management actually first appeared as part of External Server Authentication in FileMaker® Server 7 using Open Directory, Active Directory, and Local Security Groups. But the concept was more fully introduced as part of FileMaker Cloud Version 1 in 2016 that allowed the use of Amazon Accounts to authenticate to the Admin Console. FileMaker, Inc. has now extended this paradigm to allow users to authenticate to files hosted by FileMaker Server 16 by three additional sources: Amazon, Google, and Azure Active Directory.

❖ What Is Federated Identity Management?

At a core level, this is a fairly simple concept. However, its implementation does require some level of knowledge, skill, and experience. At base the owners of *one* digital asset, *e.g.* a FileMaker Pro database, can trust *another* service, *e.g.* Google, Amazon, or Azure Active Directory, to ***validate and authenticate*** a user's *assertion* of that user's *identity* and then pass that authentication to FileMaker Server. Similar to the way on-premises Directory Services work, if a user is deemed authentic and if the user has rights to access a database file, the user can connect with the Role-Based privileges associated with the user's Account.

Ping Identity is a leading player in Identity Management Services. They describe Federated Identity Management:

> Federated identity provides a secure, standard, internet-friendly way to share identity among multiple organizations and applications. Users sign on once with a standard network login or hosted authentication service. When they click a web application link, their identity is transparently and securely shared with the application, removing the login requirement. Since the organization authenticates the user and the application provider can verify the authenticity of the provided federated identity, application passwords are not needed and users enjoy "click-and-work" access to applications.
>
> Identity federation is a huge win for users, IT and the business alike. Users love federation because internet SSO enables them to use web applications as easily as internal applications while freeing them from remembering (and

[17] Decorte, Wim and Blackwell, Steven H. *Federated Identity Management OAuth Identity Providers in FileMaker 16.* (May 2017) http://fmforums.com/files/file/91-oauth-identity-providers/

> resetting) a battery of passwords. IT loves federation because it simultaneously enhances security and reduces the support burden, especially at the help desk. Business leaders love federation because it accelerates application and data sharing with customers, business partners, vendors and subsidiaries while decreasing risk and increasing regulatory compliance.[18]

Identity is the New Security.[19] Owners of data must consider several core issues regarding Federated Identity Management:

- They must trust the authentication source to be accurate.
- They must trust the authentication source to be secure.
- They must trust the authentication process to require strong credentials. This includes credentials lifecycle management and the use of multi-factor authentication where possible. SMS services and possibly biometrics[20] may not be especially good second factors for a number of reasons.
- They must trust the process that passes the authentication to the data source.

---

[18] *SAML 101,* p. 6. (Ping Identity. Denver, CO. April 2017. www.pingidentity.com) https://www.pingidentity.com/content/dam/pic/downloads/resources/white-papers/en/saml-101-white-paper.pdf

See also a webinar presented by Pamela Dingle, Principal Technical Architect at Ping. *Emerging Standards on the Identity Landscape.* https://www.pingidentity.com/en/resources/webinar-replays/emerging-standards-on-the-identity-landscape-replay.html

[19] RSA. *Identity: A Key Element Of Business-Driven Security.* (2016, Santa Clara, CA.)

[20] Developers should consult legal counsel in their respective jurisdictions regarding issues related to biometric authentication processes, especially fingerprints, and how they relate to privacy rights. See some relevant articles:

Fox-Brewster, Thomas. *LAPD Warrant Lets Cops Open Apple iPhone With Owner's Fingerprints. (* https://www.forbes.com/sites/thomasbrewster/2016/03/31/warrant-apple-iphone-fingerprints-hack-los-angeles/#63c334083074) (March 31, 2016).

Fleishman, Glenn. *Should You Disable Touch ID for your own security? http://www.macworld.com/article/3067340/ios/should-you-disable-touch-id-for-your-own-security.html* (May 9, 2016).

The Fingerprint Lock on Your Phone Isn't Cop-Proof. Bloomberg Business Week. http://www.bloomberg.com/news/articles/2016-05-11/the-fingerprint-lock-on-your-phone-isn-t-copproof (May 12, 2016.)

Dier, Arden. *Woman ordered to unlock iPhone with fingerprint. Newser.* (http://www.newser.com/story/224513/woman-ordered-to-unlock-iphone-with-fingerprint.html)

Holt, Maxine. *Security Think Tank: Proceed with caution on biometric authentication.* http://www.computerweekly.com/opinion/Security-Think-Tank-Proceed-with-caution-on-biometric-authentication (May 3, 2016.)

Owners of data must also be assured that those who have access to their data are the persons they claim to be, that credentials have not been compromised and become available to unauthorized persons, and that said unauthorized parties are not hiding in the data covertly.

The entire topic of credentials is an important one for developers and FileMaker Server administrators to consider. All three of the new Identity Services use web browsers as their gateway for users to verify and to authenticate their identity assertions.

Web browsers are inherently vulnerable applications. Moreover, **they permit the caching and saving of credentials for specific sites.** These include the three Identity Service gateways. So FileMaker Platform developers and server Administrators must assess the risks to their systems and data of having **unattended access points in user browsers *with stored credentials*.** Developers have no control over the behavior of these browsers in this regard. This is somewhat similar to situations where users have stored credentials in the KeyChain or in the Credentials Manager, or even of Single Sign-On options. The workstations or mobile devices of these users must be protected against unauthorized access. **Such unfettered and open devices could provide unexpected access to the FileMaker Server hosted databases using the stored credentials.**

❖ Why Use Federated Identity Management?

There are striking business use cases that argue for the adoption of Federated Identity Management. Radiant Logic is another one of the leading players in the Identity Management Services arena. Radiant notes:[21]

> More agile identity management is the key ingredient for the success of your initiatives, from the tactical to the strategic level. Whether you're adding a business unit, taking advantage of a cloud application, or orchestrating a billion-dollar merger, a flexible identity management system is purpose-built to dispatch the right people to the right applications with the adequate privileges, while guaranteeing secure access.
>
> However, actually implementing these changes can mean a host of customization pains, stalled projects, and lost opportunities. In a world of fragmented and distributed identity silos, most identity deployments lead to increased project costs, higher risks, and redundant efforts.
>
> Depending on your approach, your identity system can represent a major business and security bottleneck—or, with the right tools, it can help to accelerate the growth in your organization, add in needed agility, and bring new objectives and services within reach.

[21] Radiant Logic. *How a Federated Identity Service Turns Identity into a Business and Security Enabler, Not an IT Bottleneck.* (2016, Novato, CA. www.radiantlogic.com)

Ping Identity further notes several advantages gained by use of Federated Identity Management:[22]

- Rapid App Integration
- Instant One Click Access to improve user productivity
- Flexible Deployment of Identity Services to meet organization needs
- Accelerated Cloud Migration
- Simplification of Security Policy Administration
- Versatility in Managing Identity Data

—User Intent and Behavior—

As important as technology such as Federated Identity Management is, it likely takes second place to user action (human action). The human element is indispensible in managing security and in defining risks as part of the Risk and Threat Management process. Developers and administrators must consider the human element when designing and managing key elements of security such as Identity and Access Management and Role Definitions and Privileges. Forcepoint is a leading company advocating this approach in the Information Security field.[23]

❖ How Do I Log-in To A FileMaker Platform Database With Federated Identity Management Credentials?

Users can access FileMaker Platform by providing an Account Name and Password to the external service after first selecting the option to log-in to the database by using that service, as shown in Figure 4 below. This process can also work with WebDirect™ in Version 16 as shown in Figure 5, also shown below.

[22] Ping Identity. Webinar: *Make IAM A Business Enabler Not A Barrier.* (March 7th 2017, Denver, CO. www.pingidentity.com)

[23] Forcepoint. *The Human Point. An Intersection Of Behaviors, Intent & Critical Business Data* (2017. Austin, TX. www.forecepoint.com) See also a video presentation by Forcepoint CEO Matt Moynahan at the 2017 RSA Conference. https://www.youtube.com/watch?v=tirhsz1iezI

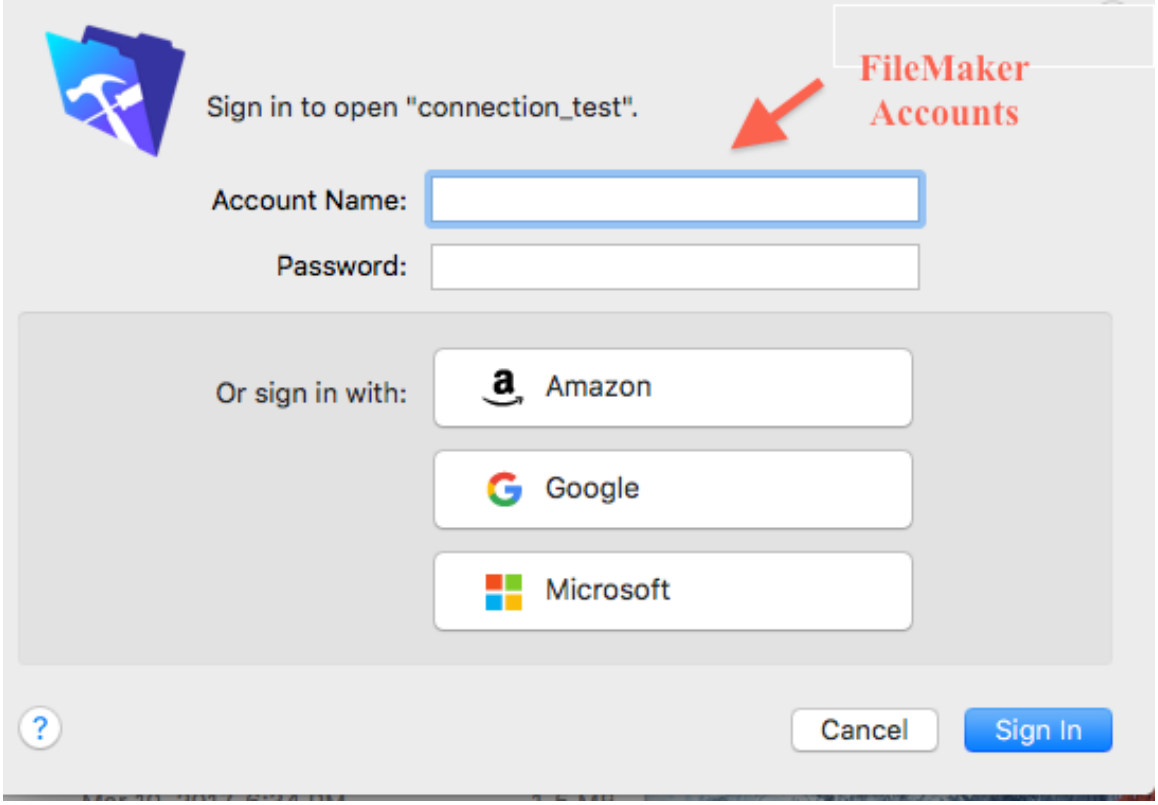


Figure 4. Log-in options using FileMaker Pro client.

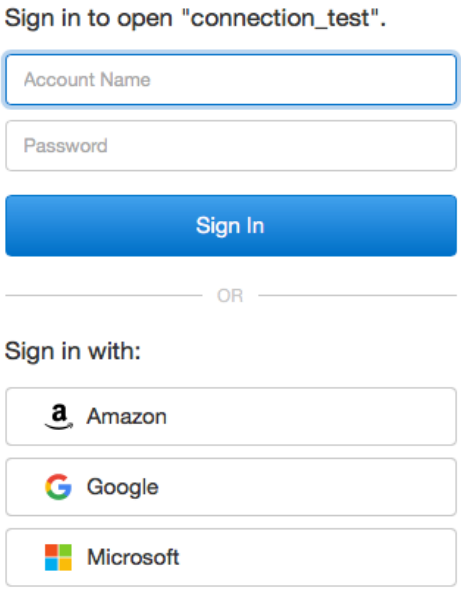


Figure 5. Log-in from WebDirect™ similar to FileMaker Pro clients.

In either scenario, a user can elect the standard FileMaker Pro Account Name and Password, including the legacy external services. Alternatively, the user can request authentication by one of the three *new* external services. Assuming that the user selects Amazon as the log-in option, the following window (Figure 6) will appear:

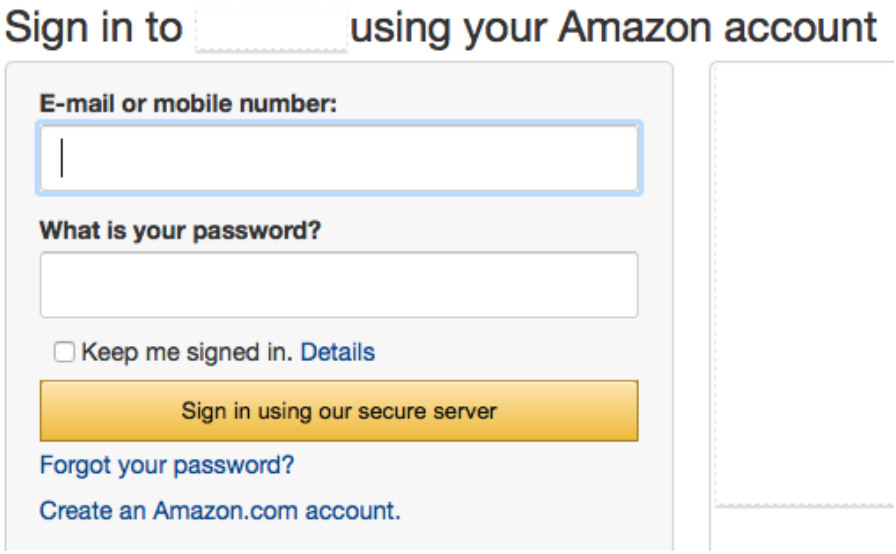


Figure 6. Amazon does the authentication and passes result to FileMaker Server.

Finally, when creating Accounts in FileMaker Pro files, developers select the option they wish to use for authentication as shown in Figure 7:

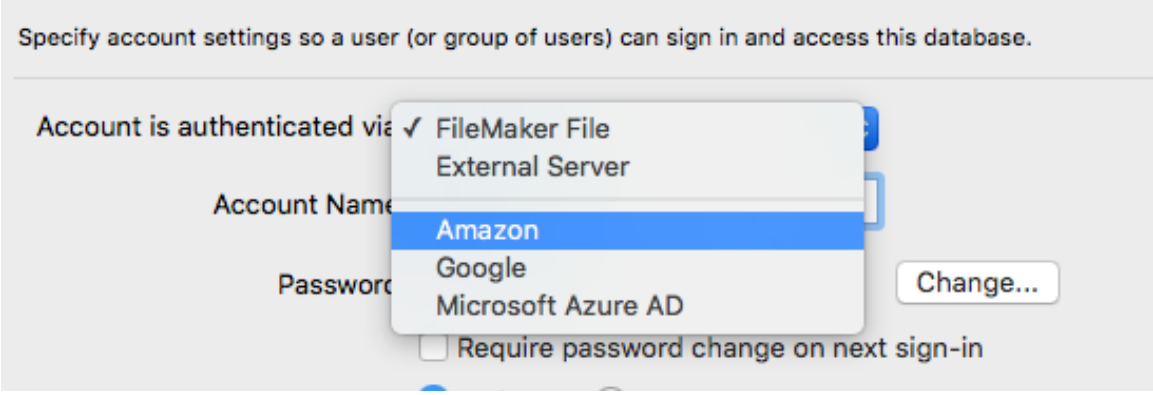
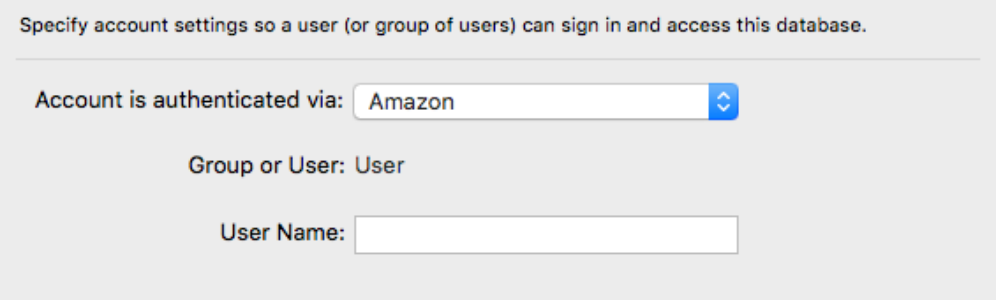
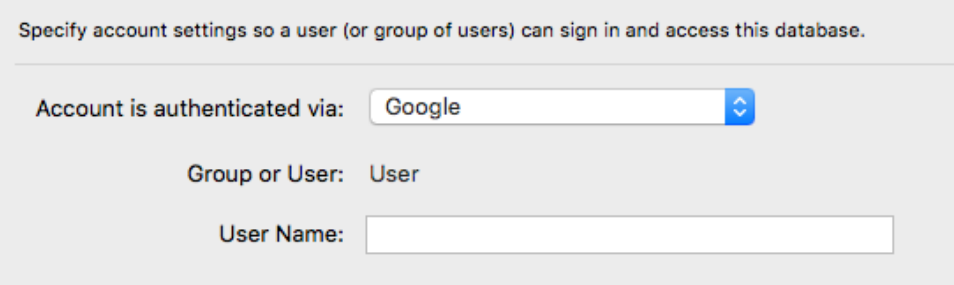


Figure 7. Selecting an authentication option in the database file.

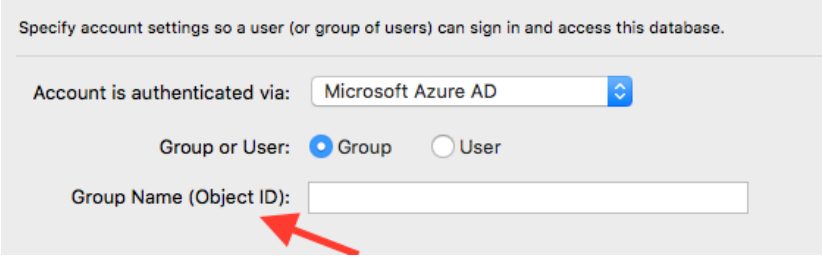
Selecting one of these will produce a second window for the respective service as shown in Figure 8 for adding the Account or Group to the database.



Amazon



Google



Azure Active Directory. (Note this can be a User or a Group)

Figure 8. Adding OAuth2 Accounts to the database file.

❖ What Are The Advantages Of Doing This?

This type of authentication allows the FileMaker Platform to leverage a number of benefits not available, or not fully available, to it otherwise:

- If the external service supports Multi-Factor Authentication capabilities, *e.g.* cards, biometrics, out-of-band notifications *via* SMS,[24] *etc*. then the FileMaker platform gets to take advantage of the Multi-Factor Authentication capability.

[24] The authors **do not recommend** the use of SMS as a second authentication factor due to its inherent insecurity.

See: Rashid, Fahmida Y. *NIST is no longer hot for SMS-based two-factor authentication. InfoWorld* (July 27, 2016) http://www.infoworld.com/article/3100685/authentication/nist-no-longer-hot-for-sms-based-two-factor-authentication.html#tk.twt_ifw

Also see: Graham, Keith. *NIST 800-63B: deprecating the use of out-of-band SMS for two-factor authentication* (July 27, 2016) https://www.secureauth.com/Resources/Blog/July-2016/NIST-800-63B-deprecating-the-use-of-out-of-band-SM.aspx

- Accounts can quickly be added to files by developers or FileMaker Server administrators without having to configure passwords. Users configure their own Account Names and Passwords in the External Service. FileMaker Server then links to these either directly or *via* a Group structure.[25]

To re-emphasize what we said before, developers, server administrators, and security administrators must consider at least five caveats when employing Federated Identity Management services:

1. How to enforce credentials life-cycle management including password expirations, reusability, and deactivation.
2. How to enforce rules for credentials strength and complexity.
3. How to enforce Multi-Factor Authentication if required.
4. How to stay abreast of changes in the OAuth2 standards.
5. How to maintain persistent Internet connections to and from the Identity Services.

—IN REVIEW—

In this White Paper we have identified and introduced a number of new features and concepts related to FileMaker Platform Security in Version 16. There is another White Paper that describes and analyzes the new OAuth2 functionality in both FileMaker Pro 16 and FileMaker Server 16.

- The FileMaker Platform has a twelve-year history going back to FileMaker Pro 7 in 2004 for providing and updating new security features including:
  - Modern, industry-standard Accounts and Passwords
  - Role-Based Privileges
  - External Server Authentication using Open Directory, Active Directory, and Local Security Groups
  - Encryption In Transit
  - File Access Protection
  - Encryption At Rest
  - KeyChain and Credentials Manager storage controls
  - Blocking hosting of insecure files
- FileMaker Pro 16 and FileMaker Server 16 introduced new privilege controls to help close some previously unaddressed vulnerabilities in FileMaker Pro files:
  - AppleEvent and ActiveX API controls. APIs are now disabled by default. Developers must enable them to use them.

---

[25] For purposes of FileMaker Platform I&AM, Azure Active Directory supports Groups; Amazon and Google do not.

  - FMPURL API controls. This API is also now disabled by default. Developers must enable it to use it.

- FileMaker Pro 16 introduced new encryptions functions. They are **not part of the I&AM security schema** and **do not take the place** of *Encryption At Rest*.
- FileMaker Pro 16 and FileMaker Server 16 expanded Identity and Access Management controls using three new External Services and the OAuth2 protocol to enable Federated Identity Management:
  - Amazon Accounts
  - Google Accounts
  - Azure Active Directory Accounts, including Groups.
- Federated Identity Management offers some significant technical and business advantages to FileMaker Platform developers and users.

—ACKNOWLEDGEMENTS—

The authors wish to acknowledge the assistance of several persons in the FileMaker community for their help in reviewing this manuscript prior to its release. We wish also to thank them, both for that assistance and for their many contributions to the FileMaker Community.

- Colleen Hammersley Makin, Data-Waves, Inc.
- Maida Sussman, Blue Forest Data, LLC
- Rick Kalman, FileMaker, Inc.

—ABOUT THE AUTHORS—

WIM DECORTE is the Senior Technical Architect at Soliant Consulting, a FileMaker Business Alliance Platinum Member company. He is a leading expert on FileMaker Server, FileMaker Platform integration, and IT infrastructure issues. He is the author of numerous White Papers, Technical Briefs, and BLOG posts.

STEVEN H. BLACKWELL is a FileMaker Business Alliance Platinum Member Emeritus. He is the author of *FileMaker Security: The Book* as well as numerous White Papers and Technical Briefs about FileMaker Platform Security. He is also the creator of the FileMaker Security BLOG (http://fmforums.com/blogs/blog/13-filemaker-security-blog)