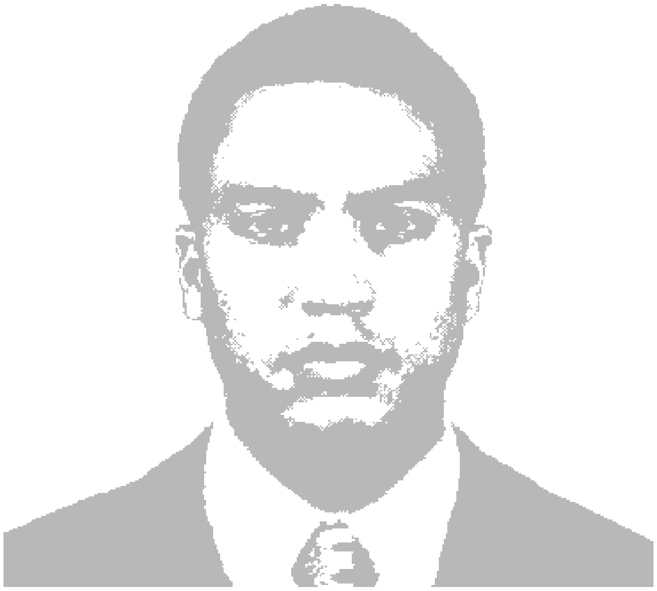
LifeFX
The Face of the Internet™

Digital Rights Management

Security and Usage Tracking for LifeFX Stand-Ins and Xpression Files

Bill Wilder
Senior Architect
LifeFX, Inc.



Digital Rights Management

Abstract

LifeFX has introduced a revolutionary new media type: life-like, talking, emoting human faces called Stand-Ins. The human face is among the most powerful ways to communicate with other people, so interest in using LifeFX Stand-Ins is high.

This whitepaper explains the LifeFX security architecture, which protects your investment in both Stand-Ins and Xpression files, and usage tracking capability. The discussion focuses on web-based Stand-Ins.

Table of Contents

The Need for Digital Rights Management

Digital media – such as video, music, and images – are ubiquitous on the Internet. The web enables companies and individuals to communicate in ways that were simply not possible before. For the first time, a person from anywhere in the world at any hour can find your web site in a search engine, visit your web site anonymously, see the incredible media content you so painstakingly created, and… steal it.

The process of controlling access to valuable assets in the digital realm is commonly known as Digital Rights Management, or DRM. While there are legal remedies for some kinds of rights violations, DRM is best enforced with technology.

If you're thinking about putting a LifeFX Stand-In on your web site, you should rightfully ask questions like these:

> *How do my users know that the LifeFX player is safe to install?*
>
> *Can Stand-Ins and Xpression files be infected with viruses?*
>
> *Can someone else change the way my Stand-In looks?*
>
> *Can someone put my Stand-In on another web site?*
>
> *Can I track how my Stand-In is being used?*
>
> *Can anyone else put words in my Stand-In's mouth?*
>
> *Can someone take an Xpression file I created and play it with another Stand-In?*

The LifeFX security architecture employs five layers of security: download, player, Stand-In, content, and authoring security. It protects your customers by providing a secured download, and it protects your digital assets by preventing their unauthorized use. Furthermore, it lets you track how your assets are used, providing both extra security and marketing data.

We designed our product line with security in mind. Our DRM solution uses sophisticated cryptography that stays behind the scenes, without compromising performance or functionality. Content authors simply need to install FaceXpress and the Stand-Ins they've purchased. Everything else happens transparently.

Download Security

The LifeFX player is a software component that can be freely downloaded and installed over the Internet. Once installed, it enables users to view life-like digital humans called Stand-Ins that move, talk, and emote. The scripts that animate the Stand-Ins, which are called Xpression files, are under the control of the hosting web site.

Web site visitors who are asked to download a software component must be guaranteed that the component is safe and secure. They need to know that an identifiable, reliable company developed the software component and that the version they are installing has not been tampered with. LifeFX complies with industry best practices for component downloads.

The LifeFX player takes the form of an ActiveX control. ActiveX is a Microsoft *de facto* standard technology for developing software components under Windows. ActiveX offers tight integration with Internet Explorer, the performance advantages of native code, and digital signing of downloads.

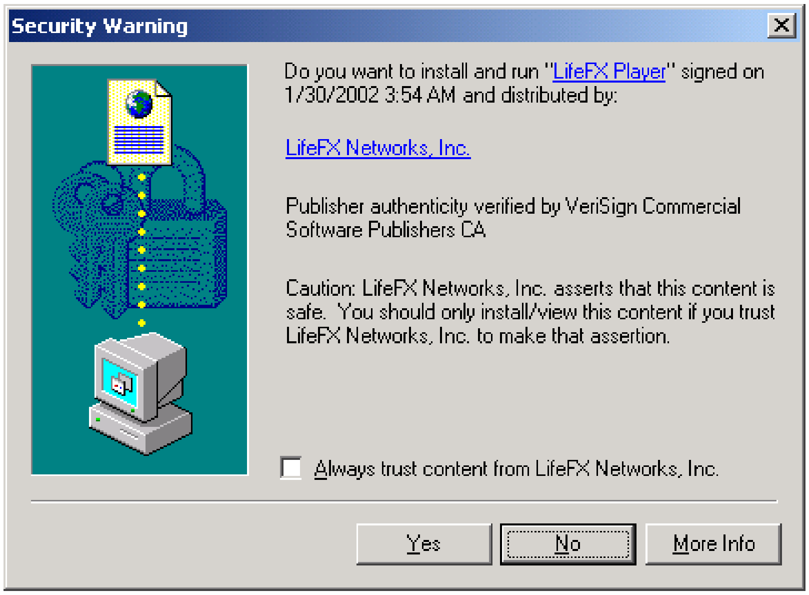
Download signing

When a user visits a web site that features an ActiveX control – like Macromedia Flash, Adobe Acrobat, or the LifeFX player – the control is not automatically installed on the user's machine. Internet Explorer always asks[1] the user to authorize the installation. This process is based on a trust model – do you trust the author of the ActiveX control? Usually ActiveX controls are distributed by reputable companies and are trustworthy. It is possible, of course, for a virus or other malicious intent to be incorporated into an ActiveX control, so users should not install controls that aren't from trusted sources.

When IE downloads an ActiveX control – as it can do when a web page refers to an ActiveX control with an `<OBJECT>` tag – it normally displays a security dialog (see Figure 1). The dialog asserts that the ActiveX control has not been tampered with and also identifies the company that created it – in this case, LifeFX. The dialog is made possible by a Microsoft technology called Authenticode, and by a digital certificate embedded in the downloaded component.

> *LifeFX digitally signs its downloads using a cryptographic key provided by VeriSign. Microsoft Authenticode technology ensures that the downloads have not been altered since LifeFX created them. This is the same approach used by Microsoft, Macromedia, Adobe, Apple, and many other companies.*

[1] This discussion assumes the user has "reasonable" security settings for Internet Explorer. Though settings are always reasonable by default, Internet Explorer can be reconfigured to ignore security concerns, thus allowing any ActiveX control to be downloaded and installed without verification. This sort of configuration is obviously unsafe and not recommended.



Do you want to install and run "LifeFX Player" signed on 1/30/2002 3:54 AM and distributed by:

LifeFX Networks, Inc.

Publisher authenticity verified by VeriSign Commercial Software Publishers CA

Caution: LifeFX Networks, Inc. asserts that this content is safe. You should only install/view this content if you trust LifeFX Networks, Inc. to make that assertion.

□ Always trust content from LifeFX Networks, Inc.

Figure 1. Internet Explorer installation dialog for an ActiveX control

Note that the user can click on the hyperlinks to read more about the control and its source. If the user does not trust the source, he or she can click No, and the downloaded code will never be run.

If the user decides the downloaded software is reputable, the installation proceeds; in the case of the LifeFX player, it takes only a few seconds. Once the software has been installed, it will not need to be installed again.

LifeFX digitally signs all of its player installation packages. Also, under some circumstances (and under the control of the content author), the player will download and install a text-to-speech engine on the user's machine. The TTS engine installer is likewise signed.

See Appendix A for an explanation of the cryptographic principles behind digital signatures. Also see the many Authenticode articles on the Microsoft and VeriSign web sites.

Player Security

As an ActiveX control, the LifeFX player exposes a unique COM interface so it can be controlled by container applications (like IE) and by scripts running within container applications (like a Javascript function in a web page).

Before IE loads the player, it always queries whether the player is Safe for Initialization and Safe for Scripting. The LifeFX player advertises that both of these operations are safe using `IObjectSafety`, a standard COM interface.

In doing so, the player is asserting it cannot be used to damage the user's computer, or compromise the user's security, no matter how a container application or a script exercises the player's interface.

The player is able to accomplish this by simply concentrating on its job: loading Stand-Ins and playing Xpression files. Its COM interface does not expose any functions that could be used for other than their intended purposes.

Stand-In Security

Stand-In security is "factory installed" – we enable it at LifeFX when we build a Stand-In. The security settings are all tested and verified before we ship you your Stand-In. All Stand-In security is enforced by the player.

Once the LifeFX player is securely installed, it is ready to load Stand-Ins and play Xpression files. If a web page calls for the display of a Stand-In that is not already available in the user's Stand-In cache, the player quickly downloads it. Stand-Ins are cryptographically protected by VeriSign digital signatures, just like the player download. However, the LifeFX player itself checks the authenticity of the signatures, so the verification happens transparently to users; no Internet Explorer security dialog is necessary.

When the player loads a Stand-In, an initial test ensures that the Stand-In is well-formed. In other words, the player ensures that the binary data is structured correctly, is the right size, and has other expected characteristics of a Stand-In. Another test checks that the Stand-In was properly signed and secured by an authorized LifeFX Stand-In factory. A corrupt or tampered-with Stand-In will fail one of the tests, and the player will refuse to load it.

> *Because the content of a Stand-In is protected by a digital signature, any unauthorized changes to the way the Stand-In looks or acts, or changes to its security settings, are easily detected. The player would detect any tampering when it started loading the Stand-In, and refuse to finish loading it.*

Stand-In security settings

Once the Stand-In's authenticity has been confirmed, the player checks its factory-installed security settings. One of these is a setting that indicates the web site domains this Stand-In is authorized to play from. For example, if the domain `lifefx.com` was authorized, this Stand-In could be hosted on any page from a `*.lifefx.com` domain such as `lifefx.com`, `www.lifefx.com`, or `any.thing.lifefx.com`. It would not, however, be allowed to run in any page under, say, `lifefx2.com`, `fakelifefx.com`, or `lifefx.nicetry.com`.

There are other security settings – Stand-In expiration date, flags to control a Stand-In's use in other classes of applications besides web pages, and a flag to disable the player's TTS (text to speech) support – but these are usually not used for web Stand-Ins. When you purchase a Stand-In, you should consult with LifeFX to choose the appropriate security settings for your application.

Usage tracking

The LifeFX player supports usage tracking for Stand-Ins. A Stand-In can be configured to log events when it loads or finishes speaking. The logged data includes the Stand-In identifier, the host domain or IP address, and some optional data you can customize with HTML on your web page. In the unlikely event that someone steals your Stand-In, their domain name will appear in the log.

The player can be configured to report every event, but this is usually not necessary. The player can simply log a statistical sample of events, e.g., every 100th load; this conserves bandwidth and may also address some end-users' privacy concerns.

The logging is implemented as an HTTP GET to any web server that you specify. Use of HTTP GET helps avoid firewall issues, maintain a very small data payload, and keep the logging transaction extremely brief. Logging has no user interface, so it is transparent to the end user. It happens on a separate thread of execution so it does not slow down the player. Logging is skipped if the computer is not online, without initiating a dialup connection.

The reporting frequency and the address of the logging web server must be specified when the Stand-In is built.

Contact LifeFX if you want to use this feature to collect market data, like the number of times customers listened to your sales pitch all the way to the end.

Content Security

When you create content – that is, Xpression files – in FaceXpress, you must associate it with a specific Stand-In. FaceXpress guarantees the integrity of your Xpression files by digitally signing them for you. In fact, FaceXpress signs Xpression files repeatedly, so that the player can verify each chunk as it is streamed to the client machine.

On playback, after checking that the Xpression file is well-formed, the player verifies the digital signature on the first chunk of the file. The first chunk is a header that specifies the associated Stand-In, so the player can then ensure that the Stand-In is authentic and licensed to play in the hosting web page or application. If any of these tests fail, the player will refuse to play the content. If any signature tests on subsequent chunks fail, the player will stop playing the Xpression file at that point.

Authoring Security

When you receive your purchased LifeFX Stand-In on a CD-ROM, it is packaged as an installable file with the extension .LFXSCI, e.g., 000000D-0000-11D4-0000-010000000000.LFXSCI. Don’t worry about the long file name; you can install it just by double-clicking on the file’s icon.

Installing the .LFXSCI file installs a cryptographic security key under your account on that machine[2]. This *private key* is essential for signing Xpression files. The corresponding *public key* is embedded inside the Stand-In, and the keys work together to provide a very high level of security. See Appendix A for more information.

> *It is not possible to create Xpression files for a Stand-In if you don’t have this private key, even if you have both FaceXpress and the Stand-In (.LFXS file extension). The* `PlayText` *(text to speech) interface may still work, unless it’s been disabled in the security settings.*

It should be apparent that the CD-ROM containing your Stand-In is very important. It is your responsibility to keep it in a safe, secure place, and only share it with trusted parties who you wish to allow to create content for your Stand-In. Note that a person who is just recording audio for a Stand-In doesn’t need access. Only a person who uses FaceXpress to process that audio into Xpression files will need access.

Conclusion

Since all of the security settings are “factory installed”, it is easy to overlook LifeFX’s comprehensive, layered approach to Digital Rights Management. You clearly don’t need to be a security expert to take advantage of DRM, but rest assured it is quietly doing its work behind the scenes.

When you invest in LifeFX Stand-Ins to represent your organization, you will never have to worry about misappropriation of your digital identity and creative content.

[2] The keys will only be accessible under the credentials of the user logged in when they were installed. It is safe, therefore, to install them on a machine supporting multiple accounts. If more than one account on the same machine needs access, Stand-Ins can safely be installed again under other accounts.

Appendix A: Cryptographic Principles

Historically, cryptography has been concerned with *privacy*: encoding (encrypting) data so that unauthorized parties can't read (decrypt) it. Modern computer cryptography has three additional concerns[3]:

Identity: knowing who data is from;

Authenticity: determining whether data been tampered with; and

Non-repudiation: proving whether the intended recipient received the data.

For the commercial applications of LifeFX Stand-Ins, identity and authenticity are critical. Ensuring privacy or supporting non-repudiation are not relevant to our current business model so are not considered further. Neither identity verification nor authenticity verification depends on encryption (though they could certainly coexist with encryption). Therefore, the LifeFX security architecture uses cryptography – but not encryption.

Asymmetric keys

Identity and authenticity are central issues for commerce on the Internet[4]. If you wish to buy a book online, how can you be sure that the credit card number you type in is really going to, say, Amazon.com, and not an imposter posing as Amazon.com? The answer lies with *asymmetric keys*[5], *Public Key Infrastructure (PKI)*, and a *chain of trust*.

Throughout most of history, all encryption worked using shared secrets – military codebooks, secret passwords, and the like. This works fine as long as the parties needing to communicate can share the secret (for example, when a ship comes back to port, a new code book can be issued). The sender uses the shared secret to encrypt a message, then the recipient uses the same shared secret to decrypt and recover the original message. Note that the shared secret between Amazon.com and you could not be the same one as between Amazon.com and me, otherwise I could eavesdrop on your business or

[3] For more detail on these topics, check out *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition* by Bruce Schneier.

[4] Privacy is also important for Internet commerce – we don't want anyone else to see the credit card we are transmitting – but is not important for applications of LifeFX Stand-Ins. Note that the same cryptographic infrastructure that enables identity and authenticity also enables privacy.

[5] For the ability to digitally sign our content, we can thank Ronald L. Rivest, Adi Shamir, and Leonard Adleman who, in 1977 at MIT, invented the algorithms we now use. They later formed the eponymous company RSA (using first initials of their surnames). Their algorithms were based on ideas outlined by Whitfield Diffie and Martin Hellman at Stanford earlier, and at Berkeley before that, where it was first suggested that keys need not be symmetric, and it might be possible for an encryption system to exist that uses keys to sign or encrypt data that are different than the keys used to verify the signature or decrypt the data.

impersonate you. Realistically, it would be impractical to have to share a secret between every two parties wishing to engage in commerce.

Cryptographic approaches that use a shared secret are said to use symmetric keys (secrets). The solution for Internet commerce is to use asymmetric keys. Asymmetric keys are a pair of mathematically related keys with these useful properties:

One key is a *public key*, which can be shared widely with anybody.

The other key is a *private key*, which must be kept secret.

The public key cannot be derived from the private key, and the private key cannot be derived from the public key.

A message can be encrypted with the public key that cannot be decrypted, except using the private key.

A message can be *digitally signed* using the private key, and can be verified using the public key. A corollary is that if a message signature verifies positively using a public key, it must have been digitally signed using the corresponding private key.

The implications of asymmetric keys are significant. Suffice it to say that virtually all Internet commerce uses this technology. If I want to send you a private message over the Internet, I could get your public key from your web site and use it to encrypt a message for you that only you (the holder of the corresponding private key) can decrypt and read. If I want to send you a message and I want you to be sure it is really from me, I can first sign it using my private key, and you can be sure it came from me if it can be successfully verified against my public key.

Public Key Infrastructure

So where do these public and private keys come from? They come packaged in a *digital certificate* from a Certificate Authority – an organization that both consumers and commerce sites agree to trust. This model is similar to that of the Registry of Motor Vehicles (RMV) which issues you a state driver’s license identification that is widely considered the definitive credential for identifying yourself to strangers. We all essentially agree to trust the RMV that they are carefully checking identities before issuing licenses; we also acknowledge that a driver’s license is not easily forged. Combined, this gives us confidence that the credential is correct.

On the Internet we trust Certificate Authorities. LifeFX, like most major Internet commerce sites, uses digital certificates (and corresponding public and private keys) from VeriSign, but other trusted Certificate Authorities work fine as well. Internet Explorer maintains a list of Certificate Authorities that it automatically trusts, and VeriSign is on that list. It is the responsibility of a Certificate Authority, when issuing a digital certificate to an organization requesting one, to confirm that they in fact represent the company. This is analogous to the RMV making sure the person requesting a new license is in fact the person listed on it.

The so-called Public Key Infrastructure (PKI) makes it safe and reliable to obtain a digital certificate (which consists of a public/private key pair), and easy to share public keys with the world. This infrastructure includes the Certificate Authority web sites, like at www.verisign.com, as well as support for programmatically accessing this information from applications like Internet Explorer.

The chain of trust

Now the chain of trust comes into play. We (consumers and Internet Explorer) trust that VeriSign has been diligent in issuing its digital certificates. If a company possesses a digital certificate from VeriSign, we trust that – as long as Internet Explorer verifies all the cryptographic details are in place – the certificate is legitimate. Once we trust the certificate, we can begin to transact business electronically in a secure environment, protected by the certificate and PKI, and the cryptographic algorithms that complement them.

The LifeFX player is signed with an Authenticode digital certificate from VeriSign; Internet Explorer uses this, along with PKI, to ensure both the LifeFX player's identity and authenticity. Once installed, the player uses the same cryptographic algorithms as IE to subsequently ensure the identity and authenticity of Stand-Ins and Xpression files.

All Stand-Ins are digitally signed at LifeFX, using a secure private key, before they are delivered to customers. The player checks this signature against a known public key whenever it loads a Stand-In.

All Xpression files are signed when FaceXpress creates them, using a unique private key that LifeFX provides to the purchaser of the Stand-In. The player checks the signature against the matching public key, which is encoded inside the Stand-In, whenever the content is played.

For verification, the player not only uses the same algorithms as IE, it uses the same underlying code: the Microsoft CryptoAPI. The CryptoAPI library is an excellent choice for LifeFX since it is among the most heavily exercised code bases in history. For every instance of commerce or secure communication that occurs over the Internet through IE, this same code ensures the cryptographic integrity of the transaction[6]. Further, since the code is already resident on all modern Windows platforms, the LifeFX player does not need to include it with its downloads.

Last modified: April 25, 2002
“LifeFX”, “LifeFX Stand-In™ Digital People”, and “FaceXpress” are trademarks of LifeFX, Inc.

[6] Whether deserved or not, Microsoft applications have a reputation for containing security flaws. This author is not aware of any security breaches ever being attributable to problems in the Microsoft CryptoAPI library level of the operating system.