SIGNiX Technical Document

UNDERSTANDING SIGNiX SIGNATURES & AUDIT TRAILS

SIGNiX TotalAudit™

CONFIDENTIAL – V2.0

January 2021

SIGNiX

Version	Author	Date	Changes
1.0	John Harris	July 2014	Initial version.
1.1	John Harris	Feb 2015	Updated to include 21 CFR 11 details.
1.2	John Harris	Mar 2016	Added 'Notary Information Added' and 'Preview Completed' events as well as updated details for 'Document Presented.'
2.0	John Harris	Jan 2021	Updated title. Added content relating to signature evidence and validation. Added additional audit trail content related to Session Started, notary, KBA and other details. Small other updates throughout.

Contents

Summary

SIGNiX is committed to providing its customers with best-in-class evidence to support documents digitally signed through the SIGNiX service. This evidence is broadly known as SIGNiX TotalAudit™ and includes the following elements:

- Standards-based digital signature applied for every signature and initial in the document adds tamper-evidence and document integrity from the first signature forward. A document 'locking' tamper-proofing signature can also be applied, locking out any change in PDF tools.
- Embedded per-document signature audit trail: Once a digital signature is applied to a PDF file, the PDF file retains all changes to the document made from that point on. This information can be viewed in the 'Signature' panel in most PDF viewers.
- Embedded per-signature document view: Every SIGNiX digital signature triggers the PDF file to retain a snapshot of what the document looked like at the point of signature. This information is completely embedded in the PDF file itself and viewable in most PDF viewers by right-clicking on a signature and choosing *View Signed Version*.
- Transaction Audit Trail: SIGNiX keeps track of every single event that takes place during a transaction. This history of 'events' can encompass processes that extend beyond a single document—it provides comprehensive data about every user, action and document in a SIGNiX transaction, even keeping track of events after a transaction has been completed.

Digital Signatures

Overview

SIGNiX employs true, cryptographic digital signatures for every signature and initial applied. SIGNiX has always understood that true digital signatures offered substantial, inherent capabilities such as independence, tamper-evidence, identification, non-repudiation, and long-term viability due to their reliance on open, published document and cryptographic standards with high security and high trust, globally. However, SIGNiX was not turned away by the complexity of the technology. Rather, SIGNiX felt that the requisite challenge was to leverage digital signatures on the back-end while allowing users to apply their signatures and initials in an intuitive, easy-to-use fashion.

Going from Paper to Electronic

When you receive a wet ink signed document what are you typically looking for? First, you may check if it was signed at all. Then, you're probably looking for the right person's name which you would expect to see on the document. You might also check to see that the document was filled out correctly, or that there are no obvious alterations. Putting all of this together can be a time-consuming process, but it's also a well-understood process.

When you receive an electronically signed document, you can still look for these items, but SIGNiX gives you tools to better understand not only the document, but also the signing process, whether the document changed, and even more evidence. But of course, you have to know what to look for.

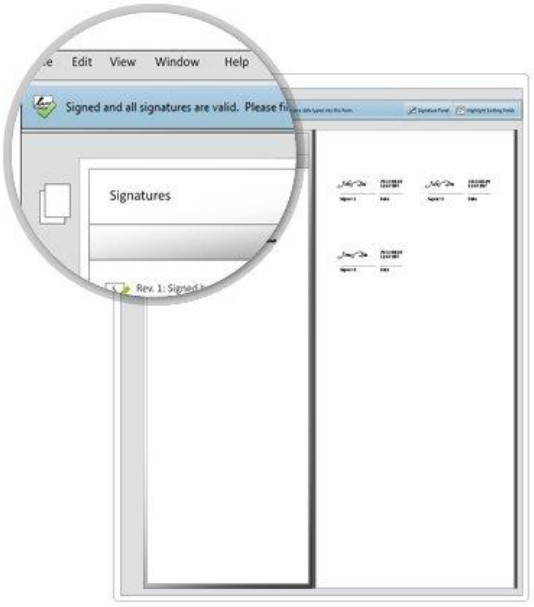
Rely on the PDF

SIGNiX produces digitally signed PDF documents. The PDF file format is well-known and is an international standard (ISO 32000-1). SIGNiX chose PDF because it is the most mature platform today supporting digital signatures. PDF first supported this technology way back in 1999, and since then has added on numerous powerful capabilities that each SIGNiX signature takes full advantage of.

When you receive a document signed by SIGNiX, first be sure you're looking at a PDF file on your computer or mobile device…not a paper copy. While a paper copy can be useful as a reference, you will see that the PDF file has numerous features and functions that help you to trust the document. If you've been given a paper copy and asked to trust it, be sure you ask for the electronic version as well and look for all of the elements described below.

To open the PDF, SIGNiX recommends you use a fully-standards compliant PDF viewer such as the free Adobe Reader. Adobe Reader on Windows or MacOS X provides the best experience when it comes to viewing digitally signed documents from SIGNiX.

You can also use the free PDF viewer applications from Nuance, Nitro and Fox-It, though some of the icons may look different than what's presented here. If you're using a mobile device, SIGNiX strongly recommends you use the free Adobe Reader app available on the App Store and Google Play store, as the PDF signatures will render differently on iOS and Android devices.



Trust the Green Checkmark

Now that you're looking at a PDF file, what's next? If you've opened the file with the free Adobe Reader, look for the green checkmark at the top of the screen:

This lets you know immediately that nothing has changed in the document since the last signature was applied to the document, and that all changes have been signed off. Note that this icon will look different in other PDF viewers, and is generally not available on mobile devices.

When should you be concerned? When you see any of the following icons:

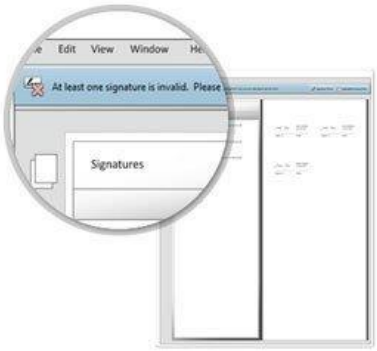
Yellow Exclamation Point

This icon is letting you know that something may have changed after the last signature was applied. Perhaps it was meant to be done, but the software is letting you know to be on notice. If you click the pen icon on the left side, you will see an in-document change tracker, showing you each of the signatures applied, and in this case, changes (such as this strike-through) made after the last signature.

Magnifying Glass

This icon lets you know that something was just changed in the document you are looking at. You will need to 'validate' the signatures for Reader to let you know what changed. Simply click the pen icon and then the 'Validate All' button. The icon should then change.

Red X



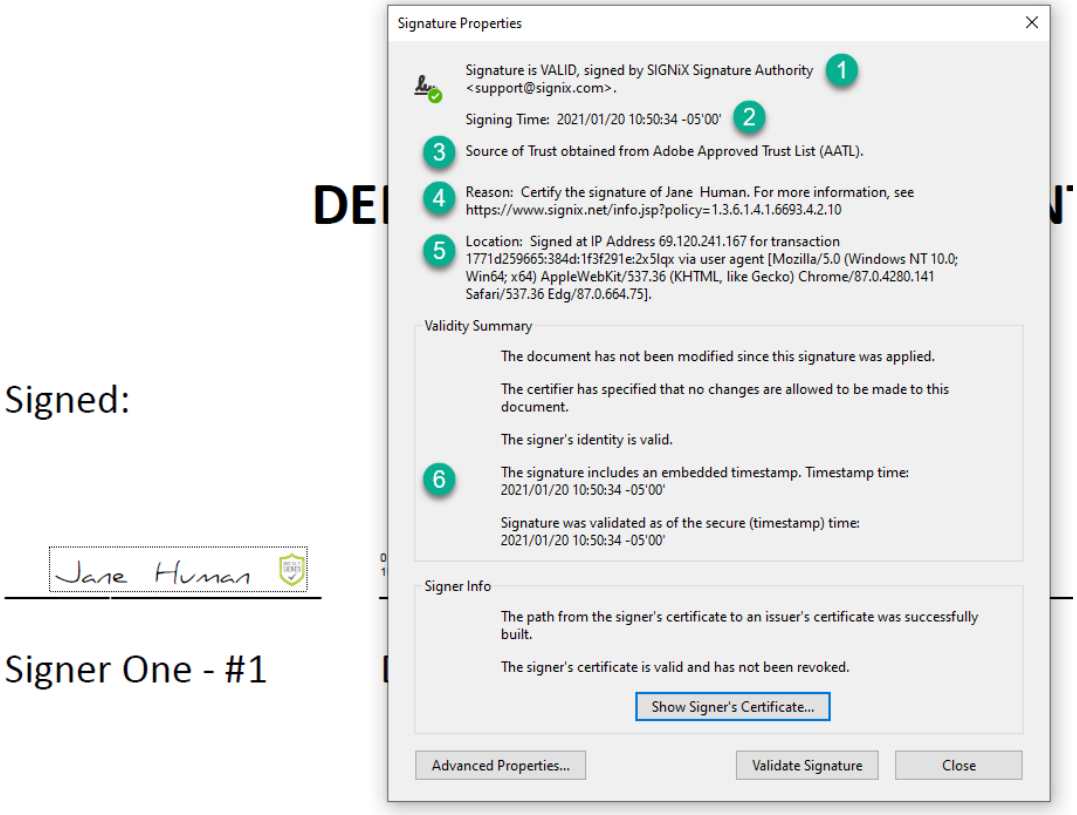
If, however, you see the Red X above, you should not trust this document. This means that substantive changes have been made to the document and the integrity of the original PDF is compromised. Get in touch with the organization or individual that sent you the document and ask for an original.

What Should the Signature Look Like?

The digitally signed document you received might have one signature or twenty. What do you need to look for in regards to the signatures themselves?

SIGNiX signatures can come in multiple appearances, as shown here. Signers can choose from one of several signature fonts, can use their finger or mouse to draw their signature or initial, and in some cases, even upload their signature as an image.

These signatures aren't just images or pictures of a signature with a link to some third party website. Each SIGNiX signature and initial creates a tamper-evident seal on the document and embeds critical information about the signature into the document itself. If you're viewing this document in Adobe Reader or another PDF viewer on Windows or Mac, you can click on each signature to get at this information. Here are some highlights.

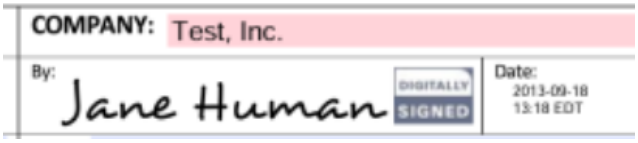


1) Signatures are represented by a digital certificate in the name of the SIGNiX Signature Authority, with an email address for support@signix.com. Older certificates may reference production@signix.com.
2) The date and time of this specific signature, including a time zone reference versus UTC.
3) The SIGNiX Signature Authority certificate is natively trusted (within Adobe products) by the Adobe Approved Trust List.[1]
4) The Reason field contains the name of the signer.
5) The location field provides the IP address of the signer at the moment of that signature, as well as the transaction identifier (DocSetID) and the 'user agent,' which is a code that signifies which browser and version were being used at the point of signature.
6) The embedded timestamp is a reference to a third party time source outside of SIGNiX to provide confidence in the time of the signature.

[1] This reference only appears within Adobe products.

In addition to the elements shown above, a SIGNiX digital signature should also display a green shield with the words Digitally Signed next to the signature image, though this alone is not enough to validate a SIGNiX signature without the additional evidence described throughout this document.

Prior to 2015, a slightly different image stating "Digitally Signed" was used to signify SIGNiX signatures.



Signature History

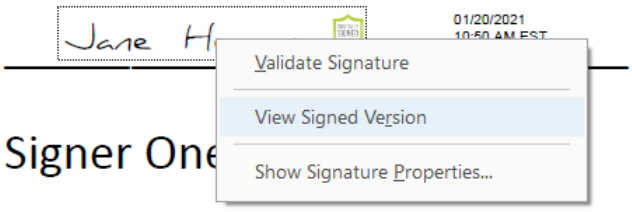
Not only does each SIGNiX signature and initial create an embedded signature on the document, it also embeds a history of the document through each signature—we call this the Signature History™. With this feature, you can easily show what the document looked like at the moment a particular signer signed the document. This is especially useful in multiple signature and party workflows where one signer may question the content of a document at the time of signature. It's available within the document, even offline.

If you have received a document with more than one signature, you can take a look at the embedded Signature History within compliant PDF viewers on Windows and Mac computers. Follow these steps:

1) Right-click (Cmd-click) on the signature in question, and choose View Signed Version.

2) The PDF viewer will create a new window displaying what the document looked like when that signer signed the document.

Viewing on Mobile Devices



Many of the advanced cryptographic capabilities of the PDF format have not yet found their way to mobile devices, so you need to be sure to understand what you can expect to see when looking at a SIGNiX digitally signed document on a mobile device. Because of a current lack of support for these features on most mobile devices, the visibility of signatures and function may differ. Some native apps may incorrectly

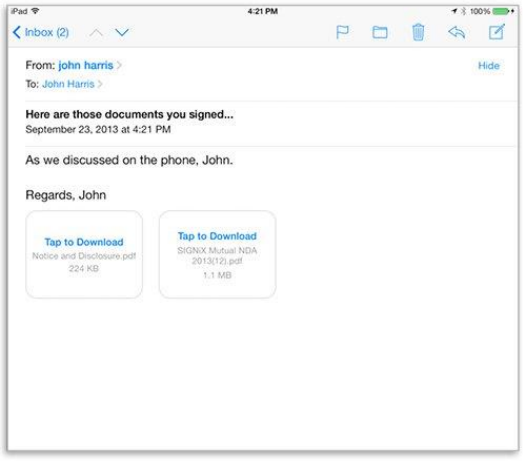
not display the signatures, so it's important to know how to view these signatures properly. Don't worry! The signatures ARE there, but the native viewer just doesn't yet know what to do with them.

SIGNiX strongly recommends installing the free Adobe Reader app for iOS or Android, as this app will correctly show the appearance of any PDF digital signature. However, note that features like the green checkmark, Signature History™ and other embedded information will not be available on a mobile device due to its more limited capabilities, so if you have questions about the document, be sure to open it on a Windows or Mac computer in Adobe Reader (or other app as described above) to dig deeper into these other assurance features.

Once you've installed the app, follow the instructions below to open a signed PDF in the app.

If you received the document as attachment in email - iOS

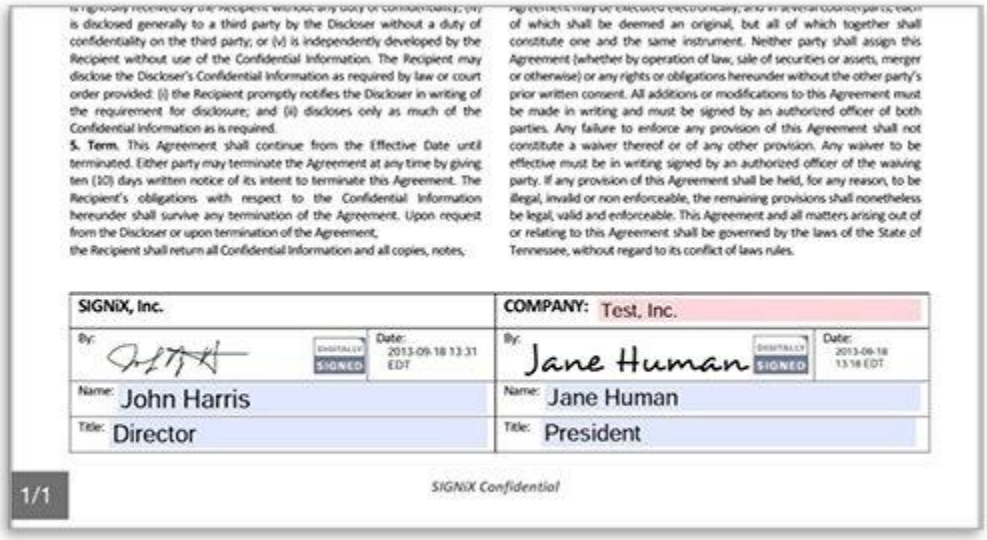
1) Scroll, if necessary to find the attachment icons. Tap to download them, if required.



2) The PDF attachment may be downloaded, or it may be previewed in-line with the email.

3) Hold your finger on the attachment icon or the previewed document until a new dialog pops-up. Adobe Reader should be one of the apps you can choose from.

4) Tap on the Adobe Reader app and the file will preview correctly, with all signatures.



If you received the document as attachment in email - Android

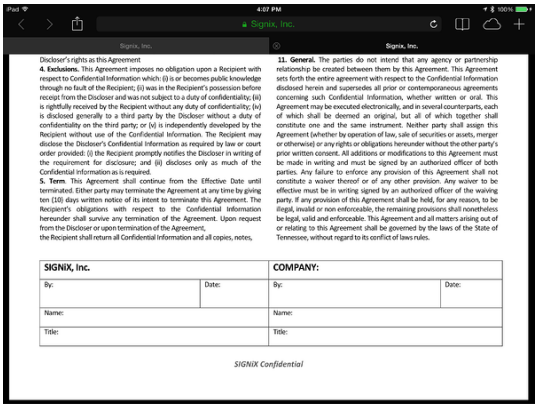
1) Scroll, if necessary, to find the attachment icons. Tap on the attachment / file.

2) When presented with the Open with, choose Adobe Reader and Always.

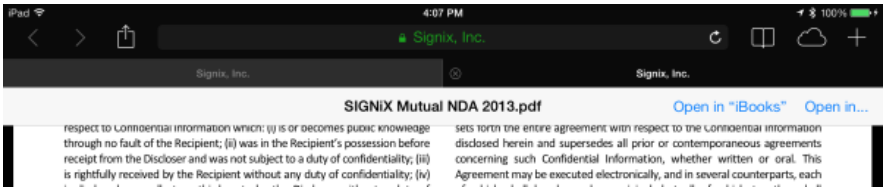
3) The file should now open in Adobe Reader and be displayed correctly, with all signatures visible.

Document already in 'preview' / Quick Look - iOS

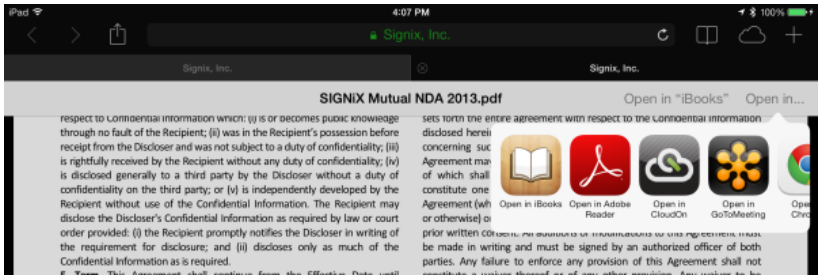
1) If you only have one attachment in an email, or you downloaded a digitally signed file, you may already be looking at the PDF. If you're in a browser like Safari, it may have opened in a new tab. You may be wondering where the signatures are…they're there, you just need to open it in Adobe Reader.



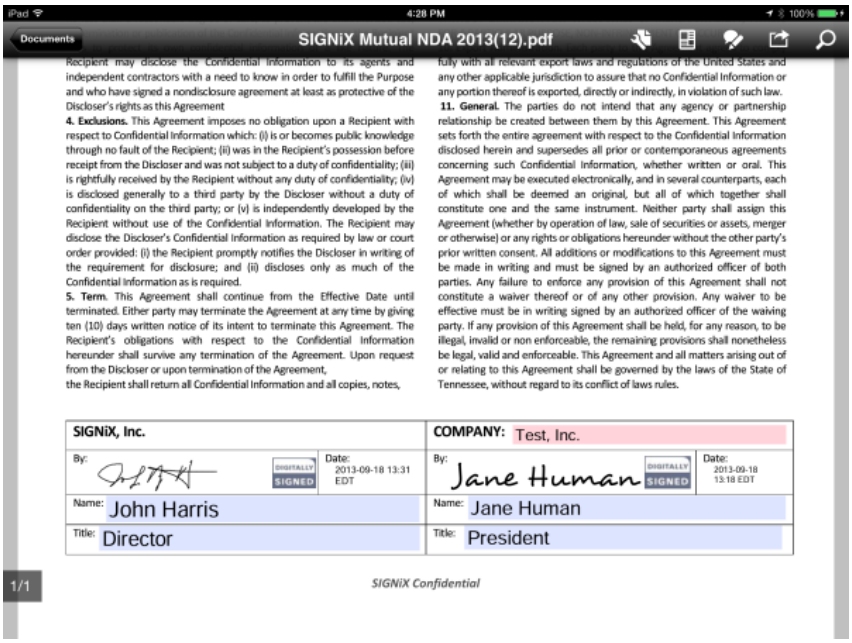
To ensure you're seeing it correctly, tap your finger once on the screen. In the upper right hand corner you should see an icon that looks like a box with an arrow pointing out of it or you may see the words Open in…



2) Tap on that icon or those words, and you'll see the following dialog.



3) Now, click on the Adobe Reader icon, and you'll see the document as it was intended with the signatures you were expecting.



Transactional Audit Trail

Overview

Now that you understand what you need to be looking for with the digitally signed document from SIGNiX, be sure that you also are able to view or access a copy of the audit trail or event history behind the transaction. SIGNiX recommends that signers in a transaction download not only the PDF versions of their signed documents, but also at least the PDF version of the audit trail.

This transactional audit trail traces every single event from the initiation of the transaction to its final steps, capturing key legal points, including transaction start, email delivery, site entry & IP address, consent, authentication result, document presentation, each signature or initial, agree/acknowledge tasks, transaction end, document presentation post-transaction and many other events. The audit trail also stores all opt out and comment activity.

Available Formats

SIGNiX provides the audit trail in different formats depending on the needs of the client and the means by which the audit trail is retrieved.

- **Digitally Signed PDF**: Parties to a transaction, as well as the Submitter, can download a PDF version of the audit trail by choosing the Download All option in the Document Review screen (for Submitters in the Status tab) after a transaction is complete. Preferred format.

- **HTML**: Submitters and administrators can also view the audit trail in a more interactive fashion via the Transaction Status tab. This is accessed by clicking on a specific transaction in the Document Center dashboard and choosing the *View History* button.
- **Certificate of Completion**: Newly available as an option in 2020, the Certificate of Completion foregoes granular detail in exchange for a shorter, more attractive format.
- **Digitally Signed XML**: Available ONLY through direct API integration with the SIGNiX service, this format can allow clients to parse the structured data in the audit trail and include it in their own reporting and analytical toolsets.

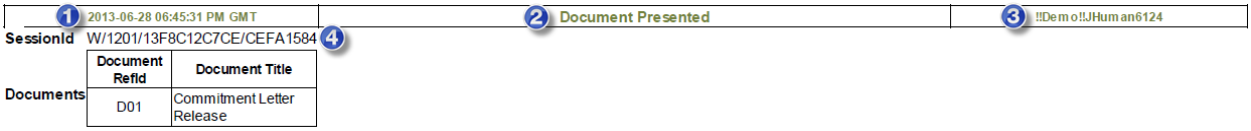
How the Audit Trail Works

Upon transaction start, SIGNiX begins collecting data about every interaction the Submitter and the Parties have with the transaction. This can include signatures and viewing, but also includes e-consent, opt outs and cancellations or changed parties. The intent is to collect as wide a field of information as possible to provide clients with an optimal set of data points to defend any and all signatures and signed documents from repudiation or challenge.

The SIGNiX audit trail is additive—that is, all changes are appended to the audit trail, not written over. Note that due to the granularity of time recording in the audit trail some events may appear to happen at the same second, but are in fact happening simultaneously or milliseconds after one another (it is possible for events happening simultaneously to be listed out of order – ie. certificate comes before the signature or vice versa when they actually happened at the same time). SIGNiX recommends that the audit trail be used alongside signed documents in a transaction to provide a complete picture of the transaction in question.

Understanding an Audit Trail Event

Below is a snippet from a sample audit trail. There are several elements to take notice of.



1. Date and time of the event, in 12h format, Greenwich Mean Time.
2. The event type.
3. The UserID of the current Party or Submitter responsible for this action.
4. Session ID

Note that for some events, such as *Email Sent*, the UserID may reflect the previous Party in the transaction. For example, in a sequential signing process, if Party A is Bob and Party B is Sarah, when Bob finished his required actions and the system sends an email notification to Sarah to let her know it's her turn to sign, the event will list Bob's UserID, as his completion triggers the email delivery to the next Party.

Audit Events, by Type

Session Started

This audit event marks when a Submitter or Party creates a secure session with the SIGNiX service. This is a critical event as it shows the IP address and the user agent (Browser) for the user as well as the *Session ID*.

2021-01-20 03:49:18 PM GMT	Session Started	Unknown
Session Id	W/1218/177207C6151/5B37EC69	
Remote IP Address	69.120.241.167	
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36 Edg/87.0.664.75	

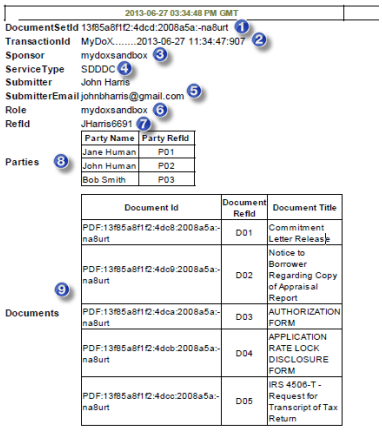
Sometimes the 'Unknown' is the UserID spot is present as the Session is started prior to the user authenticating to the SIGNiX system. In any case, the Session ID will carry through in each audit event for each event that a user takes or is party to. This allows you to track what each user does within a session.

In other words, to understand the actions a user took while they are logged into SIGNiX, follow the Session ID. For all events with the same Session ID, you know that that specific user completed them within the same secure session.

Note that if a user leaves the SIGNiX service, closes the browser, etc., they will generate a *new* Session Started event when they re-enter the service. This can allow you to track if a user access the service from a different device or different location / IP address.

Transaction Accepted by Signix

This audit event marks the beginning of a transaction and includes pertinent information as to the Parties and documents included in the transaction.


2013-06-27 03:34:48 PM GMT

DocumentSetId 13f65a8f1f2:4dcd:2008a5a:-na8urt 1
TransactionId MyDoX.....2013-06-27 11:34:47:907 2
Sponsor mydoxsandbox 3
ServiceType SDDDC 4
Submitter John Harris
SubmitterEmail johnbharris@gmail.com 5
Role mydoxsandbox 6
RefId JHarris6691 7

Parties 8

Party Name	Party RefId
Jane Human	P01
John Human	P02
Bob Smith	P03

9
Documents

Document Id	Document RefId	Document Title
PDF:13f65a8f1f2:4dc8:2008a5a:-na8urt	D01	Commitment Letter Release
PDF:13f65a8f1f2:4dc9:2008a5a:-na8urt	D02	Notice to Borrower Regarding Copy of Appraisal Report
PDF:13f65a8f1f2:4dca:2008a5a:-na8urt	D03	AUTHORIZATION FORM
PDF:13f65a8f1f2:4dcb:2008a5a:-na8urt	D04	APPLICATION RATE LOCK DISCLOSURE FORM
PDF:13f65a8f1f2:4dcc:2008a5a:-na8urt	D05	IRS 4506-T - Request for Transcript of Tax Return

1. **DocumentSetId** – A unique ID number for the transaction (aka document set) set by SIGNiX.
2. **TransactionID** – The title of the transaction as set by the Submitter.
3. **Sponsor** – Client Name
4. **ServiceType** – Standard SIGNiX service.
5. **Submitter/SubmitterEmail** – Full Name and Email Address of the Submitter
6. **Role** – Identical to Client, unless otherwise set
7. **RefID** – Referrer ID – UserID of the Submitter
8. **Parties** – Full Names of Parties in the Transaction, along with the Reference IDs for each (P01, P02…)
9. **Documents** – A list of all of the documents included in a transaction. Each document has a unique Document Id set by SIGNiX as well as a Reference ID (D01, D02…) and Document Title set by the Submitter.

Email Sent

This audit event is triggered every time an email is sent by the SIGNiX service.

2014-07-11 08:44:42 PM GMT	Email Sent	
SessionId	W/1203/147272B0532/5E4C6AD4	
Email	Party Name	Jane Human
	Email Address To	jbhdemo1@gmail.com
	Email Address From	"MyDoX Sandbox Online Signatures" <demo@signix.com>
	Body	Dear Jane Human, Your documents are available online for viewing and signing. To access your document, cli i=z0PERnF0atjL5IZtvp0Bpt PLEASE NOTE: If you are not the correct person to sign these documents, please i=z0PERnF0atjL5IZtvp0Bpt&delegate=yes If you have any questions, please contact your representative at joh
Reason	PickUp link generated for P01	

It includes the following information.

- **Party Name**: The name of the Party to whom the email is sent.
- **Email Address To/From**: The email addresses on the To and From lines.
- **Body**: The complete body text of the email, including HTML code if the email is in HTML format. (Feature added in late 2013.)
- **Reason**: Explains the nature of the email.

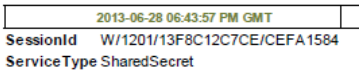
Reason codes are listed below:

PickUpEmail/ Pickup link generated for P**	This is the first email a Party will receive, letting him or her know there are documents to review and sign. This email includes the PickUp link or URL to the signing portal and transaction.
SigningCompletedEmail / Thank you mail for completing task for P**	Once a Party has completed his or her tasks in a transaction, an email is sent to thank him or her for their work.
Document set sent to the parties on the CC list	If email addresses have been added to the CC list, once the transaction is complete an email will be sent to each of these parties with all of the signed documents as attachments.
Document Set is Complete: [Transaction Name]	An email sent to the submitter when all parties have signed / completed their tasks and the transaction is complete.

Emails sent as a result of an Opt Out or Transaction Completion are not recorded in the audit trail per se, though the event itself *is* recorded.

Esign Consent Accepted

This audit event records when a user has consented to the use of electronic signatures and documents by choosing 'Accept' on the consent dialog.



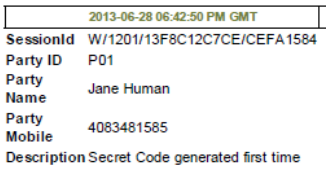
ServiceType indicates the type of authentication required for the Party.

SelectOneClick	Email or shared question and answer-level authentication
SharedSecret	Authentication via SMS text message
SelectID	Authentication via knowledge-based authentication (KBA), otherwise known as out-of-household questions.

More information on authentication types can be found in other SIGNiX documentation.

Shared Secret Code Sent

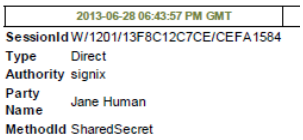
This audit event records when a random 6-digit password is sent to a Party's mobile number for authentication.



The Party ID, Party Name and mobile number of the Party (as entered by the Submitter) are listed in this audit event.

User Entered Shared Secret Code

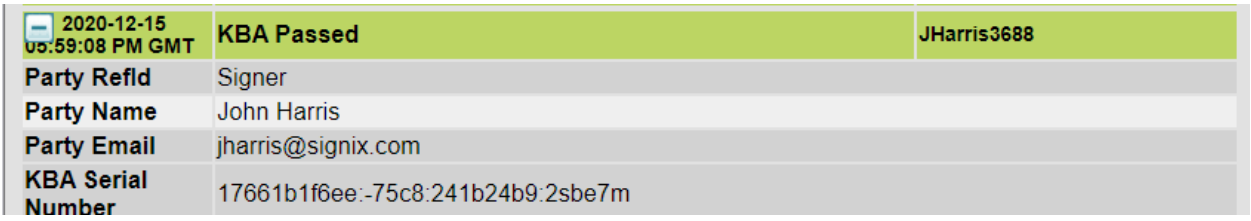
This audit event records when a user successfully enters the password sent to him or her via SMS text message (as shown in *Shared Secret Code Sent*).



KBA Events

Optionally a Submitter may choose to require signers to undergo more intensive authentication. Knowledge-based authentication (or KBA) take a name, social security number and date of birth as an input and presents the signer with 4-5 multiple choice questions based on public database information. Based on a certain number of correct answers, the signer may continue with the signing process.

Each KBA event shares the same information:



- Party RefID: Role
- Party Name
- Party Email

- KBA Serial Number: This is an internal ID for the specific KBA attempt.

Note that the UserID is present in these events, but not the Session ID, as the KBA process involves a third party identity / authentication provider.

There are numerous KBA events, including:

- KBA Passed: The KBA questions were presented and enough questions were answered correctly to pass the authentication.
- KBA No Data Returned: The system was unable to generate questions to verify the signer's identity. Most common reasons include age and/or lack of credit history, name or SSN not matching credit records, etc. If the signer has input the wrong data, they can try again, but they may be unable to proceed further if the information is correct.
- KBA Additional Questions Generated: If allowed by the authentication options, a signer may be presented with additional KBA questions to answer if they correctly answer a subset of the initial KBA questions, but not all of them.

In certain cases, a successful KBA result may be followed up with an automated credential analysis (aka KBA Scan Verify). This is particularly relevant in remote online notarization (RON) transactions. There are numerous KBA Scan Verify events as well:

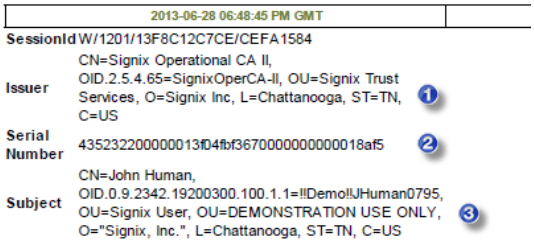
- KBA Scan Verify Attempted: The identification credential (driver's license, passport, et al) was successfully uploaded to the analysis service and is being analyzed.
- KBA Scan Verify Passed: The credential analysis was successful.
- KBA Scan Verify Failed: The credential analysis was not successful.

Certificate Issued

This audit event records the creation of the user's digital certificate and identity within the SIGNiX service for the particular Sponsor (client of SIGNiX).

Contained in this audit event are several elements that are commonly used in x.509v3 digital certificates:

1. **Issuer**: Information about the Issuer of the certificate and identity.
2. **Serial Number** of the certificate
3. **Subject** fields included in the digital certificate.



Preview Completed Event

This audit event records when a party has completed viewing all documents ahead of signature as required by the DocPreview™ capability.

Document Presented - *deprecated*

NOTE: This event is not as prominent in the new signing experience introduced in January 2015, as now ALL documents are presented to the user at the same time, rather than one at a time as was the case in the previous version of the software.

This audit event records when a document within a transaction is rendered and presented to a Party for review and action. The event lists the document Reference ID and Title.

Notary Information Added

This audit event records information that a notary party will add to a transaction during an electronic notary session, including venue, fee assessed, email of the notary party, the notary act type and then specific information regarding how parties were identified during the notarization.

2016-01-29 07:31:57 PM GMT	Notary Information Added					!!Demo!!JHarris72215n7363
NotaryPartyId	P02					
NotaryPartyName	John Harris72215n					
Venue	Alexandria, VA					
FeeAssessed	$25					
NotaryPartyEmail	jbhdemo2@gmail.com					
NotaryActType	POA					
Parties	Party Name	Party RefId	Id Method	Additional Info	Address	
	Leopold Demosmith	P01	Remote - KBA (Knowledge-based Authentication)	n/a	n/a	

Notary Seal Added

This audit event is added when a notary completes the signature associated with a specific notary seal. It includes information related to the notary's commission, including name, commission# (if applicable), state, commission expiration and the DocumentID the seal is located on.

2020-08-31 10:02:22 PM GMT	Notary Seal Added	!!Demo!!JHarris3021
Notary Name	John Harris	
Notary ID	!!Demo!!JHarris3021	
Notary Email	johnbharris@gmail.com	
Notary Commission	0000	
Notary State	State of New York	
Notary Expiration	01/01/2026	
Document Id	PDF:174450d4c44:-6b1e:-41ce8b81:2sbe7m	

User Opted Out

This audit event records when a user exits the e-signature process and chooses from a selection of options to explain why he or she is leaving the process. The event itself records the reason why and the explanation, if the user provided one. The various options and results are explained in more detail in the ***SIGNiX Exit E-Signature Options*** document.

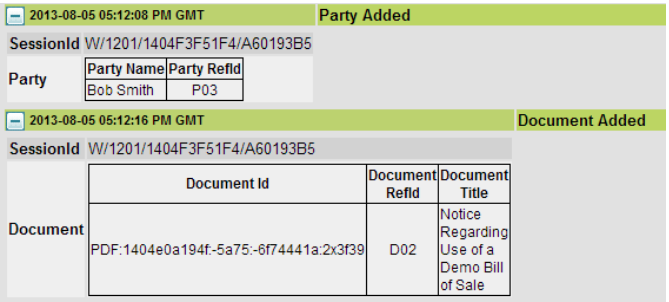
Transaction Completed

This audit event records when all Parties have completed their required actions on the documents within a transaction and the workflow is complete. Note that the audit trail will continue to record Parties accessing and viewing the documents even after transaction completion.

Transaction Suspended / Resumed

A Submitter can at any time suspend and then resume a transaction. This is often done to change a faulty email address or add a new party or document to a transaction. This audit event records when the transaction was suspended / resumed.

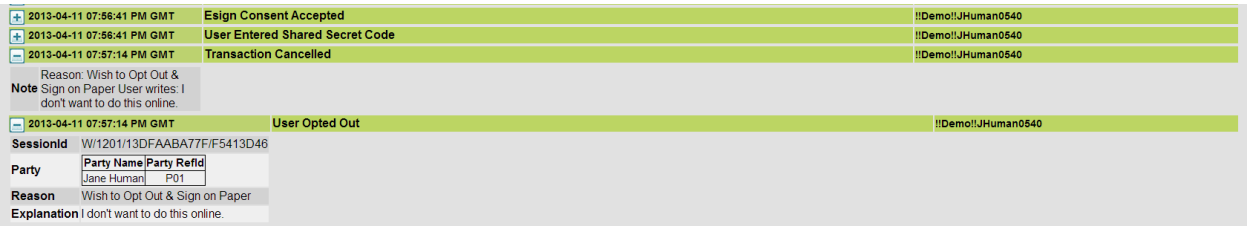
Party (Document) Added and Party (Document) Deleted



After a transaction has been started, it is possible that a Submitter may suspend a transaction in order to change aspects of the workflow. This might include adding or deleting documents or Parties in a transaction. These audit events record the addition or deletion of Parties and/or documents by the Submitter. The information of the Party or document is included in these audit events.

Transaction Cancelled

This audit event records when a Transaction is cancelled either through Submitter action, a Party opting out, or natural expiration of the transaction. The only additional information recorded for this event is in the case of a user choosing an opt out that automatically cancels the transaction.

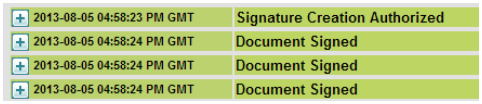


CONFIDENTIAL - ©2021

Signatures on the Audit Trail

Depending on the type of authentication chosen by the Submitter for a particular Party, different signature modes are activated. For higher levels of authentication—for example, SMS text message and KBA—SIGNiX uses so-called 'intent' signatures, where users are required to re-enter their Signing PIN when they sign a document to clearly communicate their intention to execute the document or terms in question. For these types of signatures, there are three specific audit events recorded for EACH signature or initial: *User Entered PIN*, *Signature Creation Authorized*, and *Document Signed*. This represents the input of the Signing PIN, the clicking of the 'Click Here to Sign' button, and the actual cryptographic digital signature itself.

For lower forms of authentication—email verification and shared Q&A—SIGNiX uses a simpler signing process that does not require the entry of a Signing PIN for each signature. For these signatures, only two events are recorded for each signature: *Signature Creation Authorized* and *Document Signed*. In fact, if a Party has multiple signatures on the same document, *Signature Creation Authorized* will be recorded once and *Document Signed* as many times as there are signatures or initials on the document.



In the example to the left, a document has been signed three times by the same party. *Signature Creation Authorized* is listed once, but *Document Signed* is listed three times.

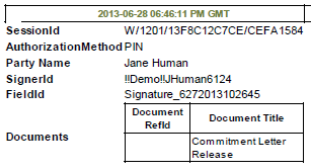
Signature-specific audit events are described below.

User Entered PIN

This audit event records when a user enters his or her Signing PIN to authorize a digital signature. Some authentication options will skip this step.

Signature Creation Authorized

This audit event records when a user specifically authorizes the creation of a signature by clicking the Click Here to Sign or related controls.

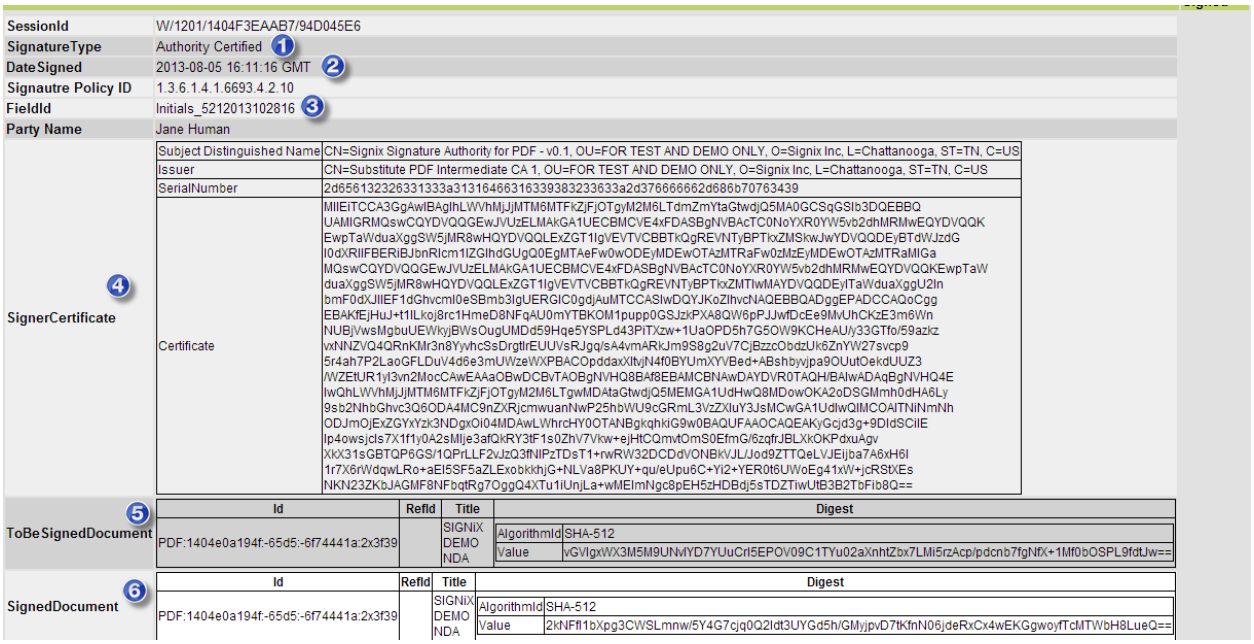


The audit event includes the following information:

- **Party Name**
- **SignerId** – The User ID of the Party
- **FieldID** – The ID number associated with the specific PDF signature field.
- **Documents** – The information relating to the document being signed.
- **Reason** – Specific to FDA 21 CFR 11 workflows. Displays the reason for the signature, and also whether it was chosen by the signer or the submitter.

Document Signed

This audit event records when SIGNiX actually digitally (cryptographically) signs a document.



SessionId	W/1201/1404F3EAAB7/94D045E6
SignatureType	Authority Certified (1)
DateSigned	2013-08-05 16:11:16 GMT (2)
Signautre Policy ID	1.3.6.1.4.1.6693.4.2.10
FieldId	Initials_5212013102816 (3)
Party Name	Jane Human

SignerCertificate (4)

Subject Distinguished Name	CN=Signix Signature Authority for PDF - v0.1, OU=FOR TEST AND DEMO ONLY, O=Signix Inc, L=Chattanooga, ST=TN, C=US
Issuer	CN=Substitute PDF Intermediate CA 1, OU=FOR TEST AND DEMO ONLY, O=Signix Inc, L=Chattanooga, ST=TN, C=US
SerialNumber	2d656132326331333a3131646631633938323633a2d376666662d686b70763439
Certificate	MIIEiTCCA3GgAwIBAgIhLWVhMjJjMTM6MTFkZjFjOTgyM2M6LTdmZmYtaGtwdjQ5MA0GCSqGSIb3DQEBBQ UAMIGRMQswCQYDVQQGEwJVUzELMAkGA1UECBMCVE4xFDASBgNVBAcTC0NoYXR0YW5vb2dhMRMwEQYDVQQK EwpTaWduaXggSW5jMR8wHQYDVQQLExZGT1IgVEVTVCBBTkQgREVNTyBPTkxZMSkwJwYDVQQDEyBTdWJzdG l0dXRlIFBERiBJbnRlcm1IZGlhdGUgQ0EgMTAeFw0wODEyMDEwOTAzMTRaFw0zMzEyMDEwOTAzMTRaMIGa MQswCQYDVQQGEwJVUzELMAkGA1UECBMCVE4xFDASBgNVBAcTC0NoYXR0YW5vb2dhMRMwEQYDVQQKEwpTaW duaXggSW5jMR8wHQYDVQQLExZGT1IgVEVTVCBBTkQgREVNTyBPTlxZMTIwMAYDVQQDEylTaWduaXggU2In bmF0dXJlIEF1dGhvcmI0eSBmb3IgUERGIC0gdjAuMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCgg EBAKfEjHuJ+t1ILkoj8rc1HmeD8NFqAU0mYTBKOM1pupp0GSJzkPXA8QW6pPJJwfDcEe9MvUhCkzE3m6Wn NUBjVwsMgbuUEWkyjBWsOugUMDd59Hqe5YSPLd43PiTXzw+1UaOPD5h7G5OW9KCHeAU/y33GTfo/59azkz vxNNZVQ4QRnKMr3n8YyvhcSsDrgtlrEUUVsRJgq/sA4vmARkJm9S8g2uV7CjBzzcObdzUk6ZnYW27svcp9 5r4ah7P2LaoGFLDuV4d6e3mUWzeWXPBACOpddaxXltvjN4f0BYUmXYVBed+ABshbyvjpa9OUutOekdUUZ3 /WZEtUR1yI3vn2MocCAwEAAaOBwDCBvTAOBgNVHQ8BAf8EBAMCBNAwDAYDVR0TAQH/BAIwADAqBgNVHQ4E IwQhLWVhMjJjMTM6MTFkZjFjOTgyM2M6LTgwMDAtaGtwdjQ5MEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly 9sb2NhbGhvc3Q6ODA4MC9nZXRjcmwuanNwP25hbWU9cGRmL3VzZXIuY3JsMCwGA1UdIwQlMCOAITNiNmNh ODJmOjExZGYxYzk3NDgxOi04MDAwLWhrcHY0OTANBgkqhkiG9w0BAQUFAAOCAQEAKyGcjd3g+9DIdSCiIE Ip4owsjcls7X1f1y0A2sMIje3afQkRY3tF1s0ZhV7Vkw+ejHtCQmvtOmS0EfmG/6zqfrJBLXkOKPdxuAgv XkX31sGBTQP6GS/1QPrLLF2vJzQ3fNlPzTDsT1+rwRW32DCDdVONBkVJL/Jod9ZTTQeLVJEijba7A6xH6l 1r7X6rWdqwLRo+aEI5SF5aZLExobkkhjG+NLVa8PKUY+qu/eUpu6C+Yi2+YER0t6UWoEg41xW+jcRStXEs NKN23ZKbJAGMF8NFbqtRg7OggQ4XTu1iUnjLa+wMElmNgc8pEH5zHDBdj5sTDZTiwUtB3B2TbFib8Q==

ToBeSignedDocument (5)

Id	RefId	Title	Digest	
PDF:1404e0a194f:-65d5:-6f74441a:2x3f39		SIGNiX DEMO NDA	AlgorithmId	SHA-512
			Value	vGVlgxWX3M5M9UNvlYD7YUuCrl5EPOV09C1TYu02aXnhtZbx7LMi5rzAcp/pdcnb7fgNfX+1Mf0bOSPL9fdtJw==

SignedDocument (6)

Id	RefId	Title	Digest	
PDF:1404e0a194f:-65d5:-6f74441a:2x3f39		SIGNiX DEMO NDA	AlgorithmId	SHA-512
			Value	2kNFfl1bXpg3CWSLmnw/5Y4G7cjq0Q2Idt3UYGd5h/GMyjpvD7tKfnN06jdeRxCx4wEKGgwoyfTcMTWbH8LueQ==

This event contains significantly more information than most audit events, as it is a cryptographic record of each signature or initial. The event lists the following information:

1. **SignatureType**: Indicates the type of SIGNiX digital signature used. 'Authority Certified' is the default signature type. 'PDF Field Lock Signature' represents a tamper-proofing signature added after all other signatures have been applied. The latter is an *invisible* signature.
2. **Date Signed**: Time and date of the signature in GMT, 24h time.
3. **FieldID**: The ID number associated with the specific PDF signature field.
4. **SignerCertificate**: Includes all of the information regarding the digital certificate used to sign the document, including the hash (fingerprint) of the certificate itself.
5. **ToBe SignedDocument**: The unique DocumentID and title of the document being signed, as well as a hash / message digest / fingerprint of the document being signed prior to signing.
6. **SignedDocument**: The unique DocumentID and title of the document being signed, as well as a hash / message digest / fingerprint of the document being signed after signing.

NOTE: If **SignatureType** is "PDF Certifying Signature" and **SignedDocument** Title is "Audit Trail," this event displays information about the digital signature on the PDF audit trail itself associated with the transaction.

Endorsement Tasks (Agree/Acknowledge) on the Audit Trail

Depending on the type of authentication chosen by the Submitter for a particular Party, different processes are followed to record so-called endorsement tasks (I Agree / I Acknowledge). For higher levels

of authentication—for example, SMS text message and KBA—SIGNiX uses a so-called 'intent' process, where a user is required to re-enter their Signing PIN when they agree to or acknowledge reading a document to clearly communicate their agreement or acknowledgement. For these types of endorsement tasks, there are two specific audit events recorded for EACH endorsement task: *User Entered PIN* and *User Acknowledged Viewing Document*. This represents the input of the Signing PIN and the actual Agree/Acknowledge step.

For lower forms of authentication—email verification and shared Q&A—SIGNiX uses a simpler endorsement process that does not require the entry of a Signing PIN for each signature. For these tasks, only one event is recorded for each endorsement: *User Acknowledged Viewing Document*.

User Acknowledged Viewing Document

This audit event records when a user agrees to or acknowledges viewing a document presented to him or her.

2013-06-28 06:51:05 PM GMT	User Acknowledged Viewing Document	!!Demo!!BSmith2851

SessionId W/1201/13F8C12C7CE/CEFA1584

Party Name Bob Smith

Documents

Document Id	Document RefId	Document Title
PDF:13f85a8f1f2:4dc8:2008a5a:-na8urt		Commitment Letter Release

The event contains the Party Name as well as the Document Id, Reference ID and title of the document being agreed to or acknowledged.