SIGNIFLOW® SOFTWARE

Helping businesses across the globe to modernise.

PROCESS AUTOMATION | WORKFLOW | DIGITAL SIGNATURES | DIGITAL KYC

SIGNIFLOW®

Americas | Asia | Australia | Europe | Middle East | South Africa | United Kingdom

www.signiflow.com

Table of Contents

1. Executive Summary 4
1.1 About PBSA Holdings 4
2. SigniFlow 7
2.1 Background 7
3. SigniFlow Software 8
3.1 SigniFlow software – High-level architecture overview 8
3.2 SigniFlow software components 8
3.3 Security Layers 9
3.4 International Compliance 15
Data Centre Security 17
Digital Signature Security 17
Document Information 18

1. Executive Summary

This document discusses SigniFlow software and methodologies used to deliver a compliant, legally binding system that enables the digitization of paper-based processes and workflows. SigniFlow also integrates with specific and focussed solutions like Digital Onboarding Systems and KYC Factory Systems.

1.1 About PBSA Holdings

The PBSA brand

With a rich history of innovation dating back over 90 years, PBSA (formerly Pitney Bowes) is a leading customer communications company, offering software, equipment, and services to help companies improve operational efficiencies and connect with their customers in meaningful ways. The new brand "**PB**" projects a vision that incorporates **people** and **business**. Our people are focused on delivering only the highest quality business solutions, empowering business with solutions built to enrich the lives of people.

The history of SigniFlow®

In 2012, PBSA began investigating the use of cryptography to secure documentation, a journey that would take it down a path of innovation and discovery. Securing physical paper with encrypted barcodes quickly turned into embedding a personal cryptographic signature on an electronic document. The need to add a workflow engine to the mix, so that multiple people could sign a single document, resulted in the birth of SigniFlow BETA in 2014.

The system officially launched in 2015, but there was a problem. Every signer in the workflow first had to be issued with a personal X.509 digital certificate. The reason was simple, the signer's identity first had to be determined before they could sign, and then embedded in the document using their personal certificate at the time of signing. The certificate also offered additional functionality and technology (X.509) that would seal the document, making it tamper-evident. The cost per user and the time it took to enrol a new user before they could sign, was simply not feasible.

Soon after launching, a major break-through by the SigniFlow team allowed the system to use different methods for multifactor authentication, federated identity, and X.509 crypto technology using Public Key Infrastructure to overcome the challenge. SignFREE was born in 2015, meaning that users could be anywhere in the world – on almost any device with Internet connectivity – when signing documents, for free.

SigniFlow has since grown into a global, enterprise-grade PKI digital signing solution with key customers in Banking, Finance, Insurance, Legal, Health care and Public services.

Location

- South Africa (Global Headquarters) - SigniFlow (Pty) Limited – Johannesburg, SA.
- United Kingdom (Headquarters for UK, Europe and UAE) – SigniFlow Limited - Horsham, West Sussex, UK.
- United States (Headquarters for North America, South America and Canada) – SigniFlow Americas LLC – New Hampshire, USA.
- Australia (Headquarters for Australia, New Zealand and Asia) – SigniFlow APAC (Pty) Ltd – Melbourne, AUS.

SigniFlow is a subsidiary of PBSA Holdings group.

Certification

SigniFlow operates in highly regulated and complex enterprise environments.

- **ISO9001:2015 Quality Management System**
  Our operations are audited and internationally certified by TUV Rheinland Germany.
- **Credit Bureau**
  PBSA (Holding Company) is a registered Credit Bureau in terms of section 43 of the National Credit Act 34 of 2005 (South Africa).
- **IT Security Management**
  SigniFlow's key IT and compliance personnel are certified ISO27001 IT Security Management practitioners.
- **Cyber Security Certification**

  SigniFlow is a Cyber Security Essentials certified by AMPG International
- **Rapid LEI Registration Agent (RA)**

  SigniFlow is certified by RapidLEI(tm) as a Global Legal Entity Identifier RA
- **GlobalSign CA e-PKI issuing agent**

  SigniFlow is certified GlobalSign (International CA with Webtrust Certification) Enterprise PKI issuing agents and certified global partners for Africa, UK, Europe and APAC.
- **Cryptographic Service Provider**

PBSA (Holding Company) is registered with the Department of Telecommunications & Postal Services (South Africa) as a Cryptography Service Provider in terms of Chapter V of the Electronic Communications and Transactions Act, 2002.

- **Microsoft**

PBSA (Holding Company) is a Gold Certified Microsoft Partner.

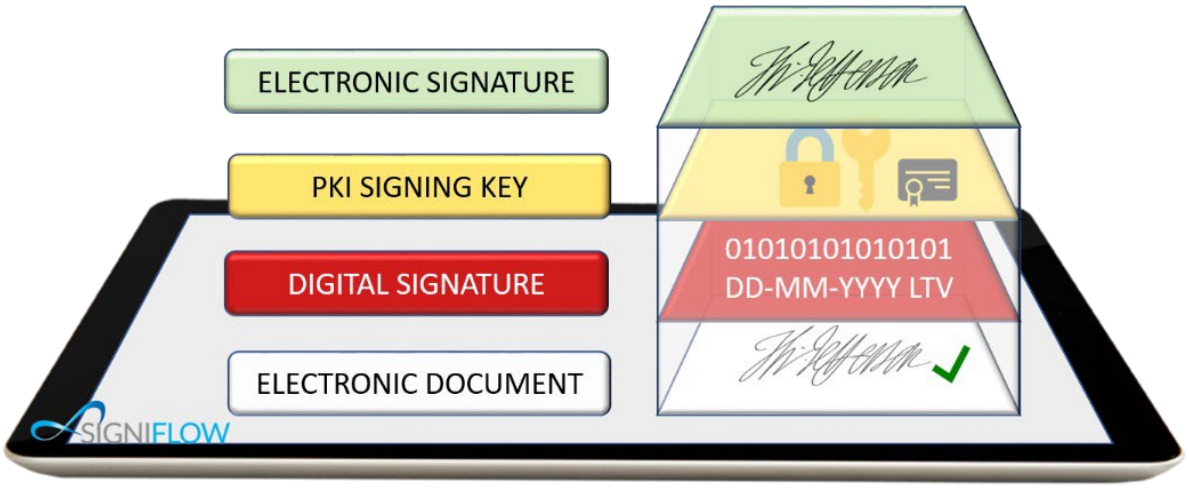
2. SigniFlow

2.1 Background

SigniFlow® is a digital signature workflow manager that enhances and fully digitises any process that requires an electronic document to be signed or approved. The solution covers anything from the most basic requirements, such as employees having to sign leave applications and their managers approving or rejecting them, to ultra-complex automated processes that require both internal and external parties to sign highly sensitive and legal documents.

SigniFlow digital signatures utilises the latest integrated personal X.509 digital certificate technologies to sign documents and embed authentication. User accounts, private keys and digital certificates are centrally created, stored, and managed in our world-class PKI with highly secure FIPS140-2 Level-3 infrastructure.

Across the world, digital signatures are fast becoming the only legally accepted replacement for handwritten signatures, because they offer inherent security - something that cannot be found in either handwritten or electronic signatures.



Digital signatures make use of a technology known as public-key cryptography. Not only does this address non-repudiation in a court of law, it also protects the integrity of documents, making them tamper evident.

3. SigniFlow Software

3.1 SigniFlow software – High-level architecture overview

SigniFlow consists of various Cloud deployments in Microsoft Azure datacentres across the world. SigniFlow has primary deployments in the United States, South Africa, Europe, United Kingdom, South America, Asia, and Australia. Although the Cloud servers are utilised for individual user accounts and small businesses, their primary function is to connect the on-premise and hosted SigniFlow enterprise deployments ("Hybrid") servers to the SigniFlow network. This enables users from any SigniFlow network, whether Cloud or Hybrid, to digitally sign documents using their private key and federated identity, no matter on which in-country Hybrid Server they emanate from.

To comply to international privacy and personal data protection laws, the regions/countries are fully segregated, meaning the data and documents of a specific region are not shared with other regions. Similarly, documents are processed and stored locally on enterprise Hybrid Server deployments in customer networks (public or private), meaning the documents are not transmitted over networks.

This is achieved with SigniFlow GUILD (Global User Interface License Directory) technology which is deployed in every region. Every customer enterprise Hybrid Server in a specific region points to the local GUILD.

Each regional GUILD in turn connects to a regional Public Key Infrastructure (PKI), which consists of software layers and network attached Hardware Security Module (HSM) infrastructure, where the cryptography operations are conducted. In some cases, customers deploy or have existing compatible PKI infrastructure, which SigniFlow uses to localise private keys and digital certificates for that client's digital signing operations.

3.2 SigniFlow software components

SigniFlow software consists of the following components that can be deployed in various installation scenarios, ranging from a single Server deployment, to Server farm deployments for high-volume transactions where each component runs separately on its own, or balanced over multiple Servers:

1) SigniFlow Applications Server/s – Requires Microsoft Server with IIS.
2) SigniFlow UI
    a. Assign UI

b. Service Oriented Architecture (SOA) Web-services JSON APIs

c. KYCFactory

3) SigniFlow Event Handler – Requires Microsoft Server with IIS.

4) DocFusion, for document template composition and document generation.

5) SigniFlow Document Management Interface (DMI) – Requires Microsoft Server with IIS.

a. Windows Service for Email and event communications.

6) SigniFlow Data storage – Required hard disk drives, SSD, SAN, NAS, etc.

7) SigniFlow database/s – Required Microsoft SQL Server.

Secure Audit - Write-Once-Read-Many (W.O.R.M) Methodology

Write-once-read-many (WORM) methodology is followed to write each time-stamped audit event as data bits, hidden in the graphic (electronic signature layer), using steganography which is then cryptographically sealed by each digital signature event. The full audit log linked to the unique document ID can be retrieved by running the PDF through a steganography decoder. (freeware)

Running any PDF signed with SigniFlow through the free SigniFlow Steganography decoder, reveals the secure, tamperproof audit trail.

The below security layers indicate the risk mitigating factors that the deployment of SigniFlow within the customers environment.

3.3 Security Layers

General Authentication process

SigniFlow Software utilizes compliant access authentication to ensure that users are verified and validated correctly. SigniFlow uses email communication to ensure the client accesses the correct system or portfolio. Using the link to access this, they will be required to sign up (First time only) to the software using their personal details, contact details, email address and mobile number.

Upon confirmation of the information, the client will be required to select a password of 8 characters or more, password must have one uppercase character, one numerical character, one special character, they are required to enter the mobile number for OTP or USSD

verification. *(optional)*

SigniFlow can reach out to clients via mobile communication methods like Whatsapp and USSD that are real time options for primary verification with fail overs to OTP.

Within the system there are other various methods such as pre-population of specific fields such as surname fields, that forces the client to fill in the balance of the data received from Customer Systems. If the balance of the data captured do not match the information shared by Customer System, the customer will not be able to proceed with the registration process.

If there is any failure on the USSD and OTP authentication, the customer will not be able to register.

Data Security

From a document security perspective, the document and the data associated to the document will rarely leave the Customers environment as it is situated in the Customers network and infrastructure. Data within a database is stored and run within the Customers environment, all maintenance on the database is carried out by the Customer on a Hybrid configuration.

The software is regularly tested, and cross checked against cross scripting and SQL injections and this is achieved by following OWASP standards for developing and deploying web applications.

Sensitive information pertaining to the user is encrypted using Triple DES.

Access to the customers environment is controlled by the customer through their VPN process when there are any changes required to their infrastructure.

Two factor Authentication

The password needs to match with the account on the system, an OTP or USSD is sent to the mobile number on the account to confirm authentication. Both methods need to pass before any access is granted to the user. This applies to the registration process too.

Encryption Layers

There are encryption layers used between SigniFlow, and customers various systems to ensure communication between the systems are secure. The below are examples of the encryption layers used:

- **"System A" Link Encryption**
  - Encryption Type: AES
  - Cipher used: AES/CFB/NoPadding

Cookies for authentication

EasiSign uses Microsoft Owin Security Cookies for user authentication and the cookies are customized to be valid for a certain time thus enhancing the security. Cookies are valid for 5 minutes on a sliding scale which means that if a user actions a request the cookie will be extended so that it expires in 5 minutes again.

Browser Security

The cookie and security are applied on a browser tab level as soon as you copy the link into a new browser or new browser tab you would need to authenticate again.

System Security

All URLs used in the browser for user navigation and emails are encrypted using a Rijndael encryption method and unique salt key.

Signature Time Stamping and Long-Term Validation

SigniFlow makes use of non-repudiation methods to ensure that our digital signatures are valid in all circumstances, our signatures are time stamped through our system. Together with all the above authentication layers it makes it difficult for anyone to repudiate the validity of the signature.

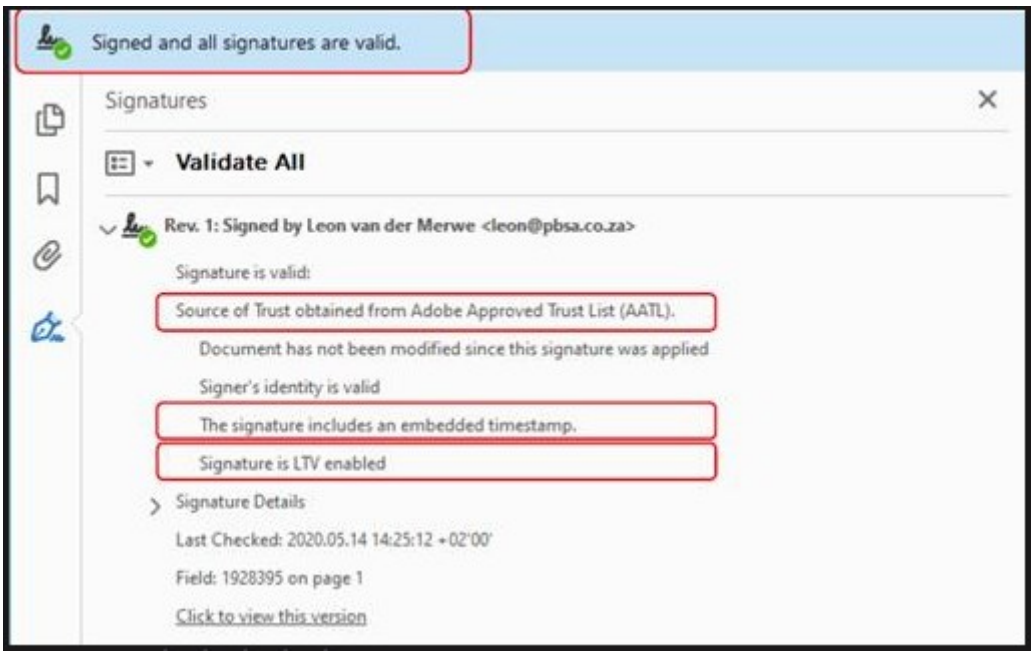
The event Audit trail is embedded in the final PDF using Adobe® standards and ISO processes. These include per-user signing versioning control, variable data filled in via SigniFlow related to the signature, TSA Timestamping per signature, Long-Term-Validation (LTV) and authentication data of the signer. These elements do not require the SigniFlow application to be validated, it conforms to the Adobe® indicators and can be validated using the latest free version of Acrobat Reader.

In addition, SigniFlow is the only digital signature application that embeds and protects each signer's audit events, using steganography and cryptography. This ensures that the audit logs embedded in the PDF are fully compliant to the most stringent measures for non-repudiation.

SigniFlow supports long-term digital signatures (LTV) and embeds the OCSP properties in digital signature. These are signatures with embedded timestamps and verification related information (VRI) such as CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol) to prove the time of signing and whether the signer's certificate was valid at the time of signing.

SigniFlow supports the following types of long-term signatures:

- PAdESPart 2 (ISO 32000-1)
- PAdESPart 3 ((CAdES-EPES)
- PAdESPart 4 (both LTV and PAdES-A signatures)



Non – Repudiation

Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if-

- a method is used to identify the person and to indicate the person's approval of the information communicated; and
- having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

There are 3 main requirements

1) Identity of the person
2) Intent of the person to electronically sign the document
3) The Integrity of the document can be guaranteed

SigniFlow handles Identity, Intent and Integrity when applying digital signatures:

- **Identity**
  - Strict, auditable methodology is followed to authenticate all users at sign-up and at the point of signing the document using multi-factor authentication.
  - Mobile number OTP (One Time Pin) or Mobile USSD.

- Email address validation.
- Username and Password

Authentication Methods that can be added (This could have an adverse effect on User experience, but the options exist):

- Geo-location (value-added not mandatory)
- Biometric validation, like facial recognition against Home Affairs photo on file (remote) or fingerprint biometrics for face-to-face.
- Digital identity – device patterns.

- **Intent**
  - A Body of evidence is produced and recorded through digital processes of positive actions that are recorded in an audit trail, for example:
    - Receiving an email from the customer describing the purpose and then clicking on the link contained in the email to fulfil the purpose
    - Receiving an USSD/OTP and actioning the USSD/OTP to open the document.
    - Opening the document, scrolling the document (perceived as reading the document) and clicking on the SIGN HERE button.

- **Document Integrity**
    - Protection of the integrity of the document by applying a digital signature using X.509 crypto-technology that embeds the identity and authentication credentials of the signer in the PDF.
    - The document is hashed, and the hash is cryptographically signed using SHA256 cryptography to embed the encrypted data in the document together with the signing time for Long Term Validation (LTV).
- **Audit trail integrity**

Write-once-read-many (WORM) methodology is followed to write each time-stamped audit event as data bits, hidden in the graphic (electronic signature layer), using steganography which is then cryptographically sealed by each digital signature event. The full audit log linked to the unique document ID can be retrieved by running the PDF through a steganography decoder. (https://update.signiflow.com/index.php/s/K57H1uaqvfaF6Ck)

A combination of the above methods, processes, audit trail and trust indicators (built into Adobe) ensures the body of evidence carries sufficient evidentiary weight to stand up in a court of Law.

- **Audit trail process**

The below audit trail process details all the events that are recorded in the audit trail within the database and the Adobe scheme. The audit trail process is applicable to a general SigniFlow process.

When the document workflow was started, and which user started the process.

Every time a user views the document it gets logged (date & time) along with the user's information.

Signing event (date & time) and browser details during signing as well as geolocation if allowed by user and IP address that the request came from.

Steganography Audit (Embedded in each signature)

- Server address where document was signed.
- Unique document ID for the document signed.
- Digital signature and certificate information gets shown on this application.
- Unique field name for every signature and user it belongs to.
- Signing events and audit up to that point.

3.4 International Compliance

The eIDAS Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions came into effect on 1 July 2016. As a European Regulation, it has a direct effect in EU law and automatically applies in the EU. The eIDAS regulation was created to simplify and standardize digital IDs and signatures across European Member States.

The eIDAS Regulation defines three types of electronic signature:

- Simple electronic signature (SES)
- Advanced electronic or digital signature (AES)
- Qualified advanced electronic or digital signature (QES)

An Electronic Signature (or Simple Electronic Signature) is defined by eIDAS as:

"data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign".

As you might expect, this means an electronic signature is any method an individual uses to 'sign' an electronic document. This covers a wide range of measures, from the simple act of affixing text or a digital image, to more sophisticated hi-tech methods which meet specific criteria set out in the regulation for advanced or qualified electronic signatures.

Electronic signatures are admissible as evidence in court. You can, in a couple of clicks, without any concrete process of identity verification or consent, have a document signed that is legally binding.

However, there is no way of guaranteeing that the document has not been modified since signing or of establishing the true identity of the person who signed. So, while electronic signatures may be legally binding, proving that the person signed the document is a whole other issue.

SigniFlow uses Digital Signatures (or Advanced Electronic Signatures), and they must meet the extra requirements set out in article 26 of the eIDAS Regulation. They are more reliably linked to the person signing the document and can detect any changes made afterwards.

SigniFlow use digital certificates and PKI (or Public Key Infrastructure) for authentication and encryption/hashing for security and its audit trail.

Based on this definition, Digital Signatures must:

- Be uniquely linked to the signatory;
- Be capable of identifying the signatory;
- Be created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- Be linked to the data signed in such a way that any subsequent change in the data is detectable.
- All electronic signatures provided by SigniFlow comply to International digital X.509 cryptographic signature standards for Advanced Electronic Signatures (AES).

Qualified Electronic Signatures are only offered by a qualified trust service provide and have the same features as advanced electronic signatures, but are created using more sophisticated technology, meet a higher standard of security, meet stricter validation criteria, and are supported by a more detailed certificate. They have the same legal effect as a handwritten signature.

SigniFlow was developed with compliance at its core and is independently certified against European Commission-recommended technology standards for all types of electronic signatures defined under eIDAS.

We utilize state-of-the-art digital cryptographic signature technology that allows you and your customers to sign documents remotely and securely, with the sound knowledge that you are signing with legally binding, enforceable signatures.

Data Centre Security

Take advantage of our Microsoft Azure hosted offerings with more than 90 compliance certifications.

MICROSOFT GOLD PARTNER	Certified competencies in Azure and Microsoft software development.	SOC 1, 2 and 3	Safeguard confidentiality and privacy of information processed in the cloud.
HIPAA & HITECH	Safeguarding individual identifiable information for the health industry.	CIS BENCHMARKS	Security standards for defending IT systems and data against cyber-attacks.
FEDRAMP	The US Federal Risk and Authorization Management Program (FedRAMP).	**Download Azure Global Compliance Infographic** 	

Digital Signature Security

Every document signed with SigniFlow has the necessary embedment's to enhance non-repudiation.

DIGITAL CERTIFICATE	All signatures are created using digital X.509standard for public key certificates.	TIME STAMPING	Timestamping is applied through a trusted Timestamping Authority (TSA).
LONG TERM VALIDATION	Embedded record of the state of the certificate at the time of signing.	TAMPER EVIDENT	Document content is protected from start to end using cryptographic algorithms.
PDF AUDIT	Full auditable X.509 trusted AATL embedments for every signer in the workflow.	AUDIT TRAIL	An automated history of events are logged against a unique document ID.
SECURE AUDIT LOG	Audit logs are written and sealed into the document using steganography.	AATL and EUTL	Supports Adobe® Accredited Trust List and European Union Accredit Trust List.
IDENTITY	Multi-factor authentication and AD, LDAP, OAuth, SAML, etc options available.	GEO-LOCATION	Embedded auditable record of the geographical location of signatories.

Document Information

Confidential Classification:

Document Contact	Document Approval
David Whitehead	Leon van der Merwe
Solutions Architect	Group CIO