ISISPAPYRUS™

Technical Documentation
General

Whitepaper

Papyrus Digital Signature Solution

Version: 1.0

Last modification: 2020-04-27

Authors:

Karsten Fischer-Vig

Roberto Anzola

ISIS Papyrus Europe AG
Papyrus Platz 1
A-2345 Brunn/Gebirge
Phone: +43-2236-27551
Fax: +43-2236-21081
E-mail: info@isis-papyrus.com
Website: www.isis-papyrus.com

Product Support:
Phone: +43-2236-27551-111
support@isis-papyrus.com

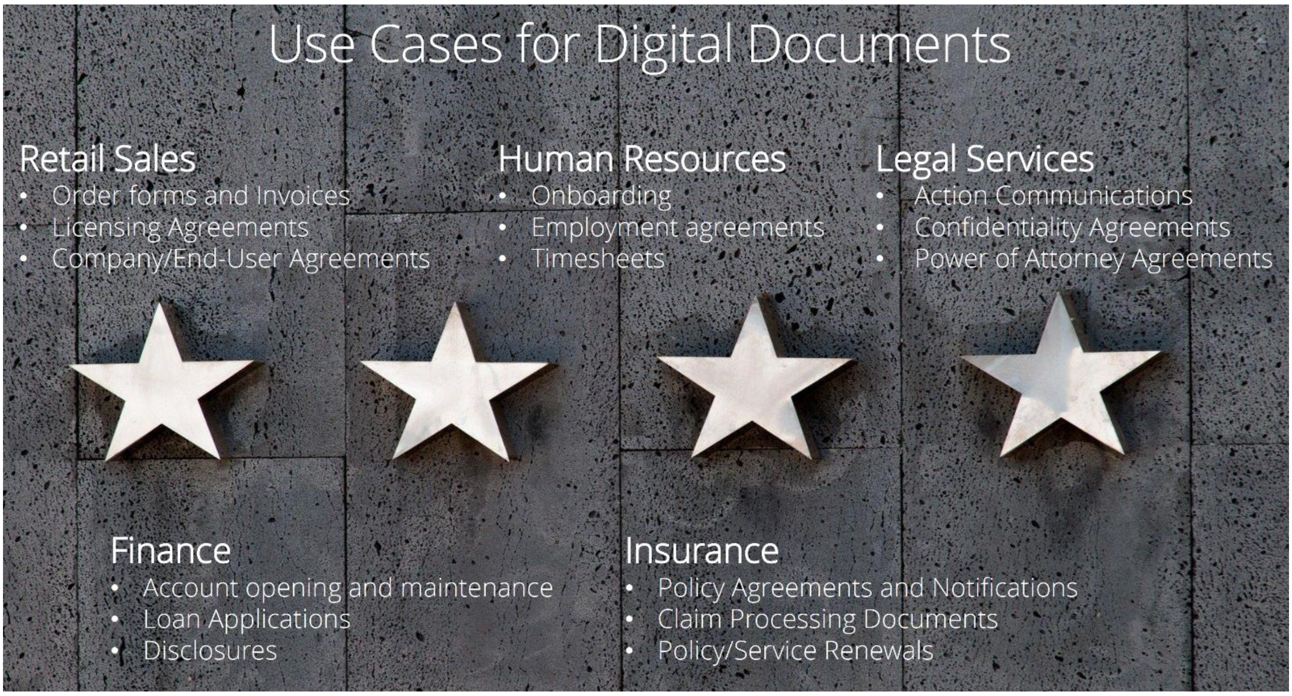
Contents

1 Introduction

Digital document signing is becoming a standard protocol, as businesses process thousands of electronic transactions each day.

Digital document signing has a lot of benefits for convenience. It is a time saver and it is energy efficient. You don’t have to meet people in person to sign a document. Also, if you receive a document that needs to be signed it unburdens you. In practice, when you digitally sign pdf documents it frees you because it prevents you from the hustle of printing the document, signing and scanning the document before sending the document.

The use cases for Digital documents and signatures is everywhere where 2 parties need to formalize and lock an agreement between 2 or more parties.



Use Cases for Digital Documents

Retail Sales
- Order forms and Invoices
- Licensing Agreements
- Company/End-User Agreements

Human Resources
- Onboarding
- Employment agreements
- Timesheets

Legal Services
- Action Communications
- Confidentiality Agreements
- Power of Attorney Agreements

Finance
- Account opening and maintenance
- Loan Applications
- Disclosures

Insurance
- Policy Agreements and Notifications
- Claim Processing Documents
- Policy/Service Renewals

The use cases span all industries and silos, both for business-to-business and business-to-consumer interactions.

2 Digital Signature Basics

In business transactions, electronic documents are being increasingly exchanged and in the same way it has been done for a long time with their counterparts in paper form. The paper documents often contain handwritten signatures, which give the documents a defined value in the applicable law.

To ensure that electronic documents can also be signed with the same legal value, the law created the electronic signature.

The advantages of electronic signatures in business processes are:

- Improved performance and quality: They enable documents to be signed and verified automatically
- Legal security: They enable an improvement of the probative value, in particular the non-repudiation of the data sent electronically.

In the legal texts the characteristics of an electronic signature are described. The texts contain no specifications for the technical implementation, however. For the technical realization the industry has developed a series of standards which define the concept of a digital signature and describe its characteristics.

How to make them Secure and Valid

Blockchain

✓ Customer Agreements, offers, communications
✓ No legal Support needed
✓ Internal Documents
✓ Amounts below certain limit

Digital Signature

✓ Contracts
✓ Legal Support needed
✓ Contract Value / Amounts over certain limit

2.1 Electronic Documents and signatures

When electronic document are being created based the need to be signed by multiple parties and locked to ensure/verify the content has been altered from what was agreed upon at the time it was signed.

2.2 Electronic Signature

An electronic signature is an electronic symbol attached to a contract or other record, used by a person with an intent to sign. In contrast, digital signatures guarantee that an electronic document is authentic.

The difference between digital signature and electronic signature is largely found in the method of identifying businesses and signers.

Digital signatures embed what’s called “Personal Key Infrastructure” (PKI) into the signing process as a way to identify both the party requesting a signature and the party providing one.

In short, PKI generates two keys, one public and one private, to uniquely identify a signer. However, both you and your signer must have a registered digital certificate from an issuing certificate authority to link the signer and their signature.

While both electronic signature and digital signature are equally capable of identifying a signer and capturing legal signatures, many consumers do not have a digital certificate, meaning they’re unable to provide digital signatures.

A digital signature, on the other hand, uses mathematical algorithms to generate a unique digital Hash. This hash, ensures the authenticity of the document, since even the slightest modification would change the hash entirely.

2.3 Digital signature

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity).

Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement electronic signatures, which includes any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures.

In some countries, including South Africa, the United States, Algeria, Turkey, India, Brazil, Indonesia, Mexico, Saudi Arabia, Uruguay, Switzerland, Chile and the countries of the European Union, electronic signatures have legal significance.

2.4 Standards for Digital documents and signatures

eIDAS created standards for the use of electronic signatures so that they could be used in a secure manner when conducting business online, such as an electronic fund transfer or official business across borders with EU Member States. The advanced electronic signature is one of the standards outlined in eIDAS.

For an electronic signature that shall be considered as advanced, it must meet several requirements:

- The signatory can be uniquely identified and linked to the signature
- The signatory must have sole control of the signature creation data (typically a private key) that was used to create the electronic signature
- The signature must be capable of identifying if its accompanying data has been tampered with after the message was signed
- In the event that the accompanying data has been changed, the signature must be invalidated

Advanced electronic signatures that are compliant with eIDAS can be technically implemented through the Ades Baseline Profiles that have been developed by the European Telecommunications Standards Institute (ETSI):

- XAdES, XML Advanced Electronic Signatures is a set of extensions to XML-DSig recommendation making it suitable for Advanced Electronic Signatures.
- PAdES, PDF Advanced Electronic Signatures is a set of restrictions and extensions to PDF and ISO 32000-1 making it suitable for Advanced Electronic Signature.
- CAdES, CMS Advanced Electronic Signatures is a set of extensions to Cryptographic Message Syntax (CMS) signed data making it suitable for advanced electronic signatures.
- ASiC Baseline Profile. ASiC (Associated Signature Containers) specifies the use of container structures to bind together one or more signed objects with either advanced electronic signatures or time-stamp tokens into one single digital (zip) container.

In the context of signing digital documents between companies and customers PAdES is probably the most commonly used throughout the world.

3 Business case for digital signatures

A number of factors must be taken into account when considering the real cost of paper-based signatures and the savings that can be achieved by using digital signatures. These factors do not just include the paper purchase, but also printing/photocopying, distributing, storage, scanning and disposal costs.

Over the last decade or so, many business have already implemented various paper-cutting solutions and streamlined their processes, however for document approval and sign-off, too often documents are still printed for gathering ink signatures. By moving to digital signatures, you can close this final gap also and achieve further cost reductions and process improvements further enabling ongoing digitalization projects.

Studies show that the total cost of handling a paper based document is ten times higher than handling the same to a digital document. The cost of paper based documents have ben seem in studies to be 15-20EUR ex. Labor cost which is actually a major component – which when included would likely double the actual cost of the paper based document compared to the digital document.

The cost of the Paper based document includes:

- Paper Purchase, Printing, Delivery, scanning, storage(archive), retrieval & disposal
- Lost time cost – it takes much longer to handle a physical document
- Fraud and compliance cost: It is easier to control and verify electronics records rather than physical
- Lost opportunity cost
- Disaster recovery back-up cost. If there is only one physical copy of important legal documents this can lead to issues if the place of storage is impacted.

And the digital document have additional features regarding safety, compliance and fraudprotection which are not possible with a paper based document.

4 Legal framework for electronics signatures

National legal requirements must always be taken into account – but in general - in terms of legal authentication, digital signatures are equivalent to handwritten signatures.

4.1 eIDAS Regulation[1]

4.1.1 Description

eIDAS oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online like electronic funds transfer or transactions with public services. Both the signatory and the recipient can have more convenience and security. Instead of relying on traditional methods, such as mail or facsimile, or appearing in person to submit paper-based documents, they may now perform transactions across borders.

eIDAS has created standards for which electronic signatures, qualified digital certificates, electronic seals, timestamps, and other proof for authentication mechanisms enable electronic transactions, with the same legal standing as transactions that are performed on paper.

The regulation came into effect in July 2014, as a means to facilitate secure and seamless electronic transactions within the European Union. Member states are required to recognize electronic signatures that meet the standards of eIDAS.

4.1.2 Vision

eIDAS is a result of the European Commission's focus on Europe's Digital Agenda. With the Commission's oversight, eIDAS was implemented to spur digital growth within the EU.

The intent of eIDAS is to drive innovation. By adhering to the guidelines set for technology under eIDAS, organizations are pushed towards using higher levels of information security and innovation. Additionally, eIDAS focuses on the following:

Interoperability: Member states are required to create a common framework that will recognize eIDs from other member states and ensure its authenticity and security. That makes it easy for users to conduct business across borders.

Transparency: eIDAS provides a clear and accessible list of trusted services that may be used within the centralized signing framework. That allows security stakeholders the ability to engage in dialogue about the best technologies and tools for securing digital signatures.

4.1.3 Regulated aspects in electronic transactions

The Regulation provides the regulatory environment for the following important aspects related to electronic transactions:

- Advanced electronic signature: An electronic signature is considered advanced if it meets certain requirements:
    - It provides unique identifying information that links it to its signatory.
    - The signatory has sole control of the data used to create the electronic signature.
    - It must be capable of identifying if the data accompanying the message has been tampered with after being signed. If the signed data has changed, the signature is marked invalid.
    - There is a certificate for electronic signature, electronic proof that confirms the identity of the signatory and links the electronic signature validation data to that person.

[1] https://en.wikipedia.org/wiki/EIDAS

    - Advanced electronic signatures can be technically implemented, following the XAdES, PAdES, CAdES or ASiC Baseline Profile (Associated Signature Containers) standard for digital signatures, specified by the ETSI.

- Qualified electronic signature, an advanced electronic signature that is created by a qualified electronic signature creation device based on a qualified certificate for electronic signatures.
- Qualified digital certificate for electronic signature, a certificate that attests to a qualified electronic signature's authenticity that has been issued by a qualified trust service provider.
- Trust service, an electronic service that creates, validates, and verifies electronic signatures, time stamps, seals, and certificates. Also, a trust service may provide website authentication and preservation of created electronic signatures, certificates, and seals. It is handled by a trust service provider.

The Electronic Signatures in Global and National Commerce Act (ESIGN, Pub.L. 106–229, 114 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch. 96) is a United States federal law passed by the U.S. Congress to facilitate the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

Although every state has at least one law pertaining to electronic signatures, it is the federal law that lays out the guidelines for interstate commerce. The general intent of the ESIGN Act is spelled out in the very first section (101.a), that a contract or signature “may not be denied legal effect, validity, or enforceability solely because it is in electronic form”. This simple statement provides that electronic signatures and records are just as good as their paper equivalents, and therefore subject to the same legal scrutiny of authenticity that

Electronic Signature Legislation

EUROPEAN UNION

Regulation (EU) 910/2014

The Regulation, better known as eIDAS,
governs electronic identification and establishes a common framework
for trust services in electronic transactions in all EU member states.

UNITED STATES

PapyrusSign is compliant with the two laws governing electronic signatures in the United States:

1. *U.S. Electronic Signature in Global and National Commerce Act of 2000 (ESIGN).*
2. *Uniform Electronic Transactions Act (UETA)*

Legality of our trust services

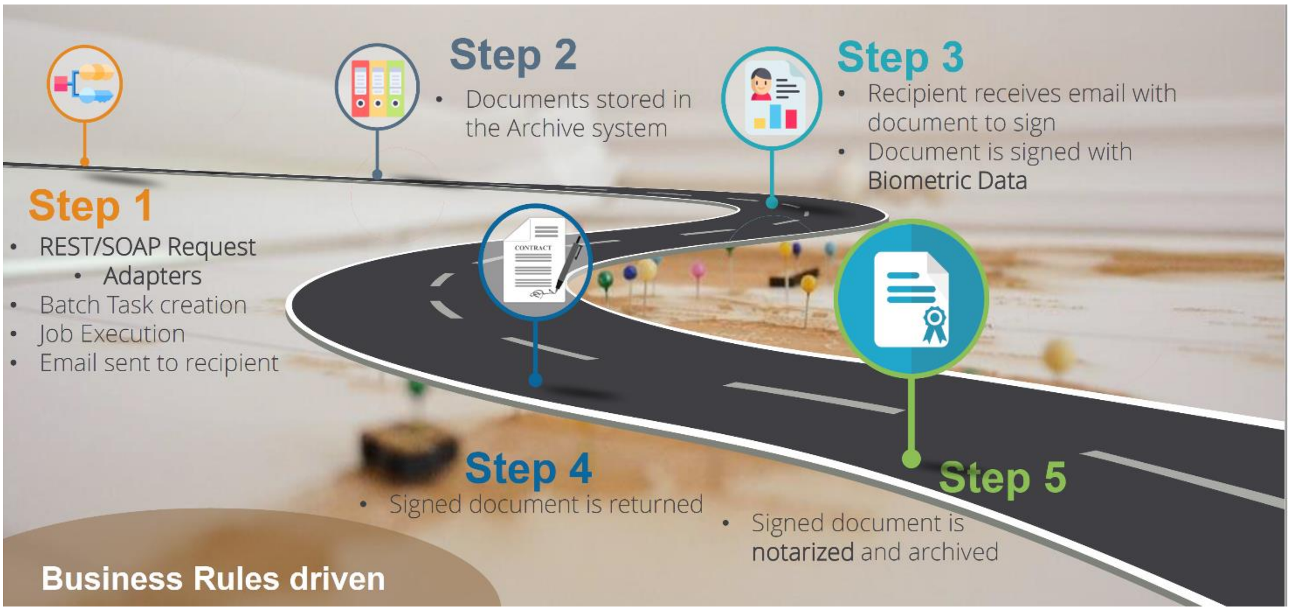
The standards above cover much of the world. Even though local laws and regulations needs to be taken into account – digital signatures in general have the same legal validity and written ones in most of the world.

5 Papyrus Digital signature technology

Papyrus Sign is an ACM-driven Papyrus Solutions allowing the definition of workflows with the possibility of combining both Blockchain Notarization and Digital Signature techniques in order to provide legal proof, trust and authenticity.

The first step on the road to working with digital signatures is to create a digital document with digital signature properties or import and enhance an existing digital document to be used with digital signatures. Papyrus can both create digital documents from data as well as import and enhance existing documents or document produced by legacy system to support digital signatures.

The data in this first step is normally transferred from business applications to Papyrus using one of the many Papyrus adapters which are available (+26 different), typically via SOAP or JSON/REST service calls in batch environments or by collecting the needed data interactively from users through the Papyrus Clients (available on Desktop, Web and Mobile) utilizing wizards which guide the user with a managed process to collect the relevant data.


Step 1
REST/SOAP Request
Adapters
Batch Task creation
Job Execution
Email sent to recipient
Step 2
Documents stored in the Archive system
Step 3
Recipient receives email with document to sign
Document is signed with Biometric Data
Step 4
Signed document is returned
Step 5
Signed document is notarized and archived
Business Rules driven

The second step typically is to store the document and data in a case or archive system where the items will be updated, tracked and version for the reminder of the process. This also provides additional tracking and auditing information about the total lifecycle of the document being managed on top of the information that is stored inside the document, auditing document, signatures and metadata created by the Papyrus Sign solution.

The third step is to collect signatures from parties which should sign the document which add electronic and/or digital signatures to the document. Electronic signatures sign as signing solutions where documents contains a handwritten signature signed on touchscreen can contain biometric information such as acceleration, pressure etc. which was use when creating the signature in addition to the image of the signature making it more individual and more resistant to fraud.

In **the fourth step** the document is returned and the case/archive is updated the document signed by all signatures.

The fifth step is to finally lock and notarize the document plus case with block chain technology making possible for all participants in the signing process to check the validity and a document against the HASH for the document in question stored in the block chain.

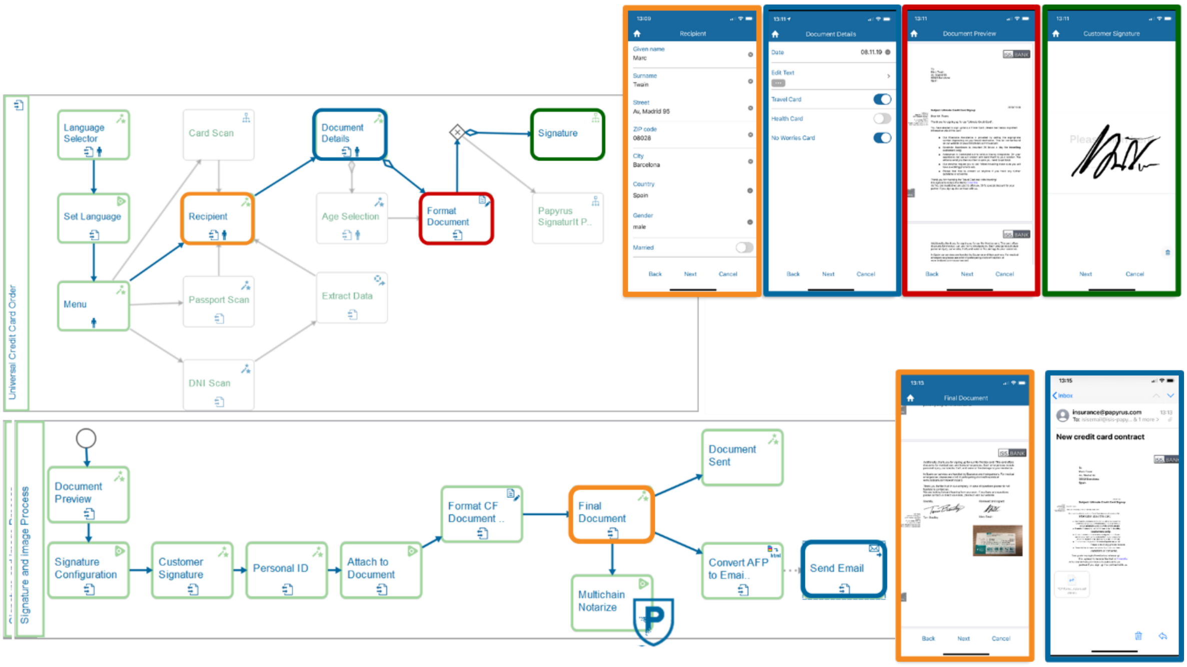
5.1 Process Integration

Papyrus Sign utilizes Papyrus ACM Framework which means that the data collection for document creation through wizards and process definition for the signing process is very flexible and easily definable by a business designer.

ACM is a highly flexible case management system that is goal oriented and not bound to strict processes. Processes are only a means to an end and non-technical business users can be empowered to adapt them to continuously changing requirements.

Knowledge workers interact with the Papyrus ACM Solution using a customizable graphical user interface. The user interface provides the same set of features regardless if accessed with fat clients (Papyrus Desktop/EYE Widgets) or thin clients (Web browser with Papyrus Desktop/HTML). This document shows all screens of the standard Papyrus ACM Solution user interface and provides step-by-step instructions for all commonly performed tasks. The standard Papyrus ACM Solution user interface is included with a Papyrus ACM Solution delivery and can be used as-is. Customer specific adaptions of and additions to the Papyrus ACM Solution user interface are not covered in this user guide.

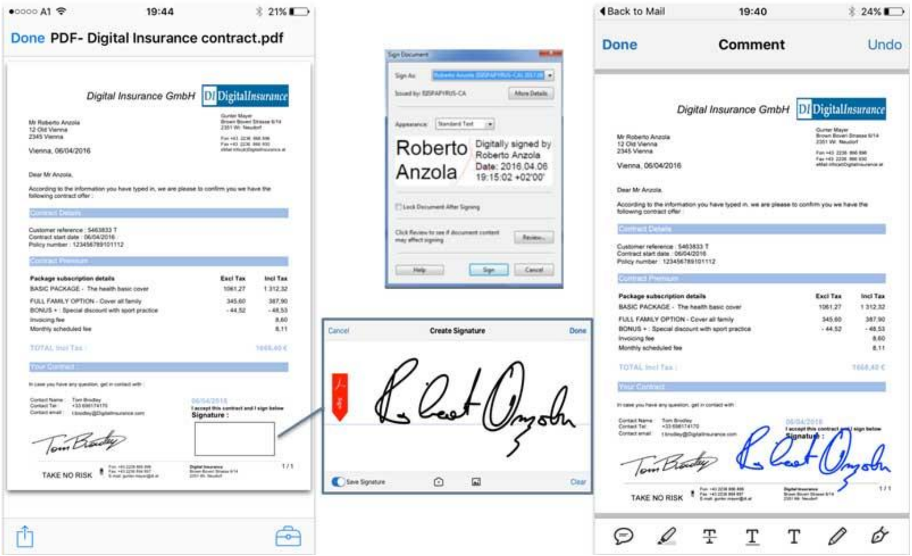
Due to very nature of ACM, it is not possible to predict a certain flow of actions for case work. It is up to the case definitions and to the decisions of the knowledge worker how work is organized.



5.2 Signatures

5.2.1 Electronic Signatures

Electronic signatures are data in electronic form which are attached to or logically associated with other data in electronic form and which are used by the signatory to sign documents or transactions. They are commonly used to sign bank, insurance, mortgage or other types of business contracts.



19:44
21%
Done
PDF- Digital Insurance contract.pdf
Sign Document
Sign As:
Issued by: ISISPAPYRUS-CA
More Details...
Appearance:
Standard Text
Roberto Anzola
Digitally signed by Roberto Anzola
Date: 2016.04.06 19:15:02 +02'00'
Lock Document After Signing
Click Review to see if document content may affect signing
Review...
Help
Sign
Cancel
Cancel
Create Signature
Done
Save Signature
Clear
Back to Mail
19:40
24%
Done
Comment
Undo

Digital Insurance GmbH

Mr Roberto Anzola
12 Old Vienna
2345 Vienna

Vienna, 06/04/2016

Dear Mr Anzola,

According to the information you have typed in, we are please to confirm you we have the following contract offer :

Contract Details

Customer reference : 5463833 T
Contract start date : 06/04/2016
Policy number : 123456789101112

Contract Premium

Package subscription details	Excl Tax	Incl Tax
BASIC PACKAGE - The health basic cover	1061.27	1 312.32
FULL FAMILY OPTION - Cover all family	345.60	387.90
BONUS + : Special discount with sport practice	- 44.52	- 48.53
Invoicing fee		8.60
Monthly scheduled fee		8.11

TOTAL Incl Tax :

Your Contract

In case you have any question, get in contact with :

Contact Name : Tom Bradley

06/04/2016
I accept this contract and I sign below
Signature :

Tom Bradley

TAKE NO RISK

1 / 1

5.2.2 Advanced Electronic signature

Advanced Electronic signatures are

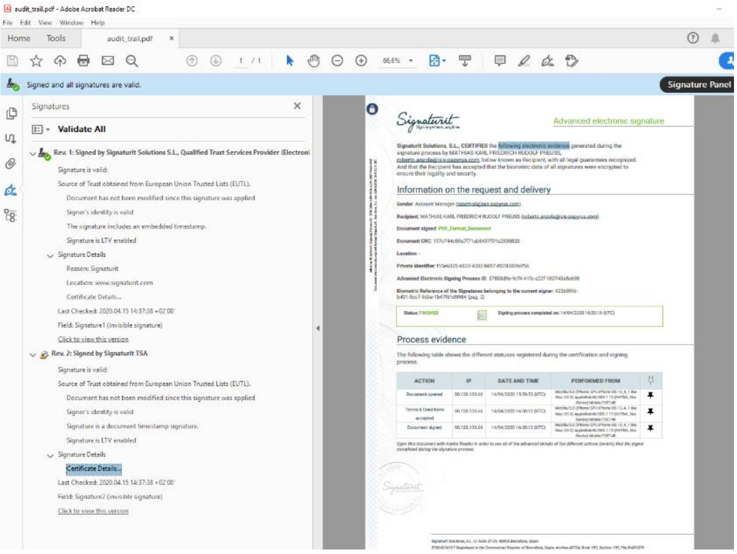
- uniquely linked to the signatory
- capable of identifying the signatory
- created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control
- linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

5.2.3 Qualified Electronic signature

Qualified Electronic signature is an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

A qualified electronic signature is an advanced electronic signature with a qualified digital certificate that has been created by a qualified signature creation device (QSCD). For an electronic signature to be considered as a qualified electronic signature, it must meet three main requirements: First, the signatory must be linked and uniquely identified to the signature. The second point is that data used to create the signature must be under the sole control of the signatory. And last it must have the ability to identify if the data that accompanies the signature has been tampered with since the signing of the message.

Qualified electronic signatures that comply with eIDAS may be technically implemented through three specific digital signature standards XAdES, PAdES and CAdES that were developed by the European Telecommunications Standards Institute (ETSI) and then need to be complemented with a qualified digital certificate.



audit_trail.pdf - Adobe Acrobat Reader DC

Signed and all signatures are valid.

Signatures

Validate All

- Rev. 1: Signed by Signaturit Solutions S.L., Qualified Trust Services Provider (Electroni
  - Signature is valid:
  - Source of Trust obtained from European Union Trusted Lists (EUTL).
    - Document has not been modified since this signature was applied
    - Signer's identity is valid
    - The signature includes an embedded timestamp.
    - Signature is LTV enabled
  - Signature Details
    - Reason: Signaturit
    - Location: www.signaturit.com
    - Certificate Details...
  - Last Checked: 2020.04.15 14:37:38 +02'00'
  - Field: Signature1 (invisible signature)
  - Click to view this version
- Rev. 2: Signed by Signaturit TSA
  - Signature is valid:
  - Source of Trust obtained from European Union Trusted Lists (EUTL).
    - Document has not been modified since this signature was applied
    - Signer's identity is valid
    - Signature is a document timestamp signature.
    - Signature is LTV enabled
  - Signature Details
    - Certificate Details...
  - Last Checked: 2020.04.15 14:37:38 +02'00'
  - Field: Signature2 (invisible signature)
  - Click to view this version

Signaturit Sign anywhere, anytime

Advanced electronic signature

Signaturit Solutions, S.L., CERTIFIES the following electronic evidence generated during the signature process by MATHIAS KARL FRIEDRICH RUDOLF PREUSS, roberto.anzola@isis-papyrus.com, below known as Recipient, with all legal guarantees recognized. And that the Recipient has accepted that the biometric data of all signatures were encrypted to ensure their legality and security.

Information on the request and delivery

Sender: Account Manager (salesmail@isis-papyrus.com)

Recipient: MATHIAS KARL FRIEDRICH RUDOLF PREUSS (roberto.anzola@isis-papyrus.com)

Document signed: PDF_Format_Document

Document CRC: 197c744c69a7f71ab8497f01e2536820

Location: -

Private Identifier: f15e6325-4833-4382-b857-d57d380b6f56

Advanced Electronic Signing Process ID: 57803d9e-9cf4-41fe-a22f-180743a5c698

Biometric Reference of the Signatures belonging to the current signer: 423b89fd-b401-8cc7-9dbe-1b47f61d9984 (pag. 2)

Status: FINISHED **Signing process completed on:** 14/04/2020 16:30:16 (UTC)

Process evidence

The following table shows the different statuses registered during the certification and signing process.

ACTION	IP	DATE AND TIME	PERFORMED FROM	
Document opened	80.120.133.66	14/04/2020 15:59:52 (UTC)	Mozilla/5.0 (iPhone; CPU iPhone OS 13_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148	
Terms & Conditions accepted	80.120.133.66	14/04/2020 16:30:12 (UTC)	Mozilla/5.0 (iPhone; CPU iPhone OS 13_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148	
Document signed	80.120.133.66	14/04/2020 16:30:12 (UTC)	Mozilla/5.0 (iPhone; CPU iPhone OS 13_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148	

Open this document with Adobe Reader in order to see all of the advanced details of the different actions (events) that the signer completed during the signature process.

Signaturit Solutions, S.L. C/ Ávila 27-29, 08005 Barcelona, Spain
[illegible] Registered in the Commercial Register of Barcelona, Spain, Archive [illegible], Book [illegible], Section [illegible], File [illegible]

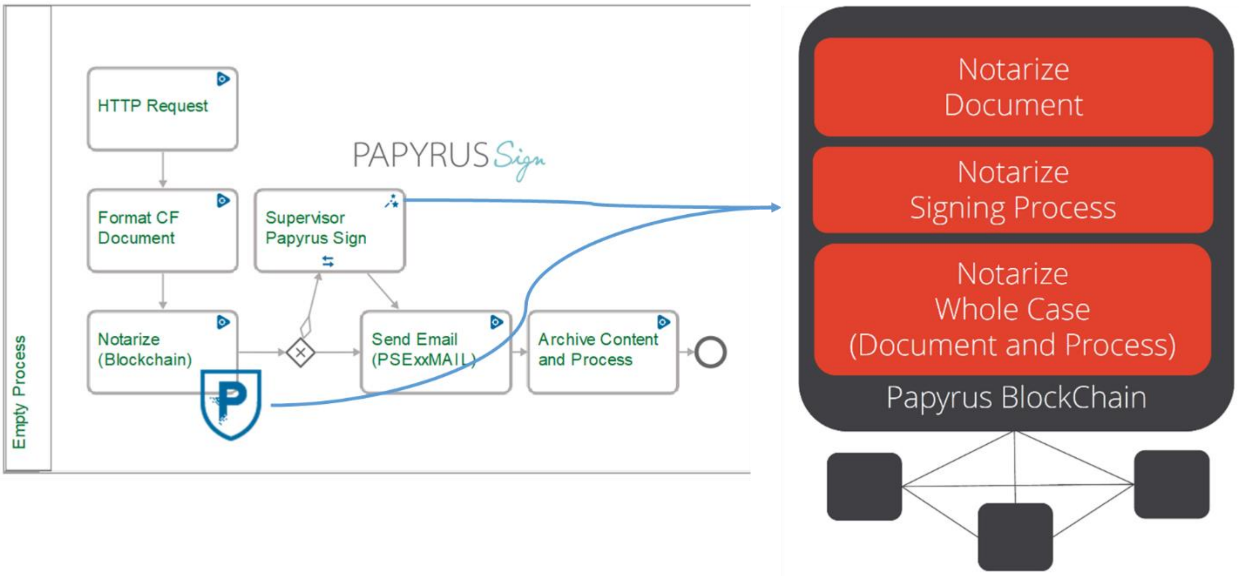
Probably the most commonly used qualified electronic signature standard in use is PAdES where some member countries have issued digital certificates to all citizens and have company versions available as well. Papyrus have implemented support for PAdES for several generations of the product.

Previously, a signatory would sign a document or message and then return it to the intended recipient via the postal service, facsimile service, by hand or by scanning and then attaching it to an email. The issue with these methods is that they are not always secure or timely. Delays in delivery could occur, and there exists the possibility that signatures could be forged or the enclosed documents may be altered. The risk increases as multiple signatures are required from different people who may be located in different locations.

These problems are alleviated by using qualified electronic signatures, which save time, are legally binding, and provide a higher level of technical security

5.3 Papyrus Block Chain

Papyrus Blockchain technology is an add-on or alternative to using established authorized electronic signature processes.



Papyrus Digital signature technology

5.3.1 Papyrus Block chain trusted documents

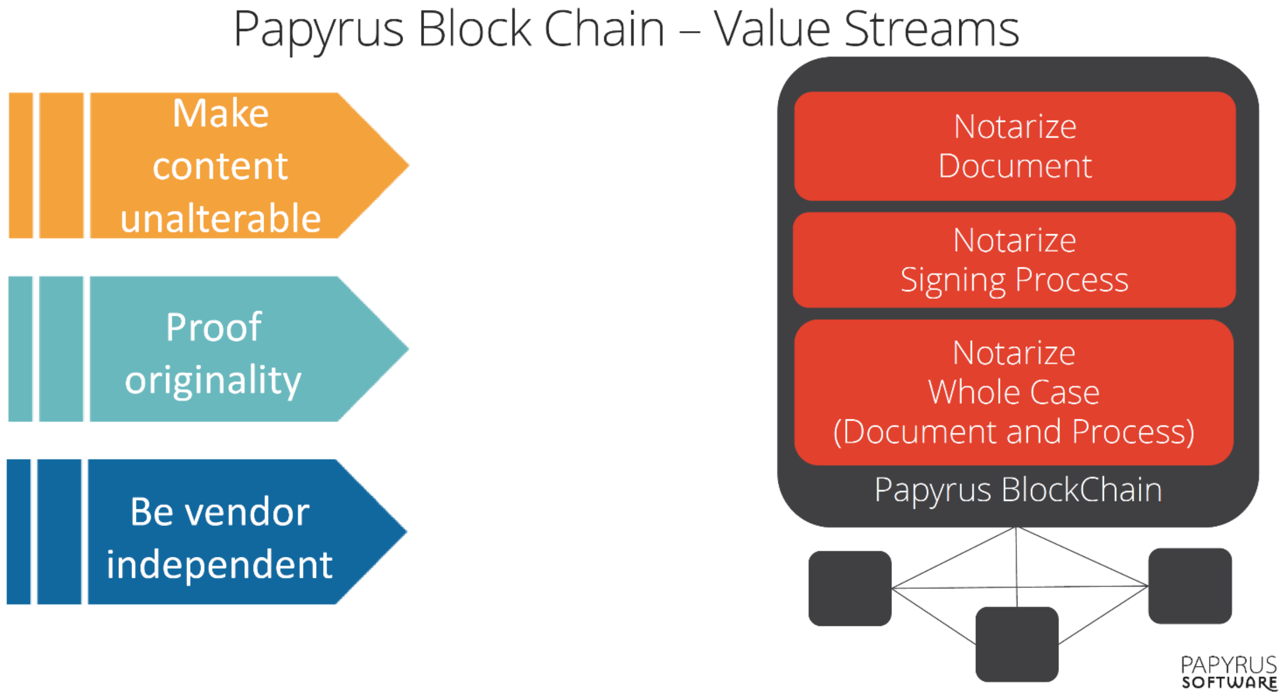
Papyrus Content Management Services are integrated with the Adaptive Case Management (ACM) Solution providing Blockchain secured documents. Blockchain ensures files which cannot be corrupted and can be audited on demand.

For Customers exploring the Blockchain applications without large capital investments in infrastructure and training, the Papyrus Blockchain Ecosystem provides the lowest-risk gateway to make the first steps with permissioned distributed private ledger technology, for a fast-track Blockchain implementation across your business.

For Customers who are already members of Blockchain ecosystems or consortiums, specific connectors are available for the most important Blockchain platforms (e.g. Multichain, Hyperledger Fabric, …).

Main features:

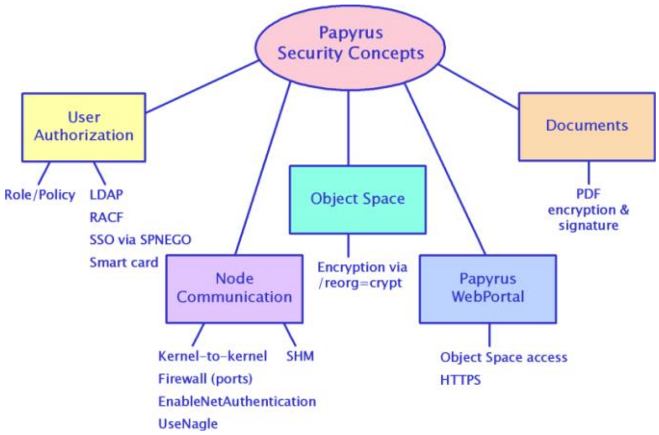
- Adaptive Case Management integration
- Cloud test environment for your evaluation of the Papyrus Blockchain Ecosystem.
- Prototype, Test, and Build Blockchain powered notarization applications for documents
- Develop Blockchain extensions for existing applications



Blockchain	Digital Signature
P	PAPYRUS Sign
Papyrus Blockchain guarantee the originality of a document or any content/message or process. It has a different legal value than electronic signature. It does not use a trusted legal authority.	The Papyrus Sign® Solution is recognized as a trusted legal authority as it uses - and relies for the legal authentication - the signature placed in the document by a recognized trusted legal entity in most of the countries in the world..

5.4 Integrated Security Concept in the Papyrus platform

Security does not have to be implemented as an additional external solution or through integration efforts. All processes, documents and data are safeguarded by a system of user roles and privileges. Users are authenticated by log-in which can be optionally augmented with SmartCard or fingerprint technology. Documents and processes can be digitally signed for subsequent auditing.



All parts of the Papyrus platform access, storage and communication are designed with security in mind.

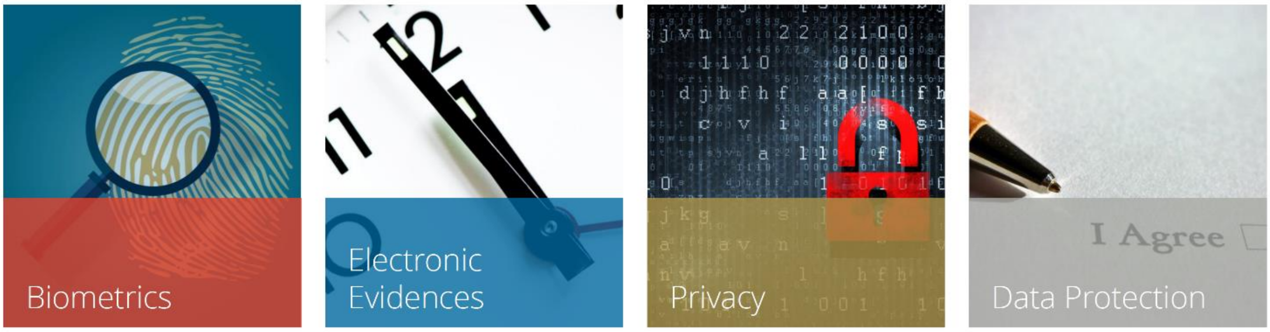
Papyrus Security standards V7:

Functionality	Algorithm	Explanation	Comments
SSL protocol	TLS 1.3	TLS Version 1.3.	Used for all HTTP(S) communications (choosing cipher suite during handshake to get the best security supported from both sides)
Key Agreement	ECDHE	Diffie-Hellman with Elliptic Curve and ephemeral keys	industry standard
Authentication	RSA	RSA with 1024 bit keys	only internally in the node2node authentication and key exchange used
Block Cipher	AES256	AES with 256 bit keys (longest possible key)	used if encryption of object space is enabled also part of TLS handshake
Blowfish	128 bit	Data encryption	only internally used in node2node communication, will be replaced by AES256 in newer versions
Password store	SHA2-256	Additionally salted	Used for user password store
Checksums	SHA1-160	First algorithm	Only internally used in node2node communication, will be replaced by better algorithm in newer version
User authentication	SSO	Single Sign On with Kerberos, SPNEGO or LDAP(S)	Security as the operating system provides, OpenID connect (based on OAuth 2.0)

prototype for Google authentication available

The following security concepts are implemented in Papyrus:

Authentication	-	Ensure that a user is identified with certainty
Confidentiality	-	Encrypt the document and data transmissions
Authorization	-	Control what someone can do with a document or workflow
Accountability	-	Track what someone did
Authenticity	-	Verify the originality and source of an action
Auditing	-	Being able to create a full compliance record



Biometric data on the signer's handwriting

- Speed
- Pressure
- Acceleration

Collect electronic evidence during the signing process in a substantiating Document

- To ensure its integrity with a qualified time stamp

Firewalls and encrypted communication.

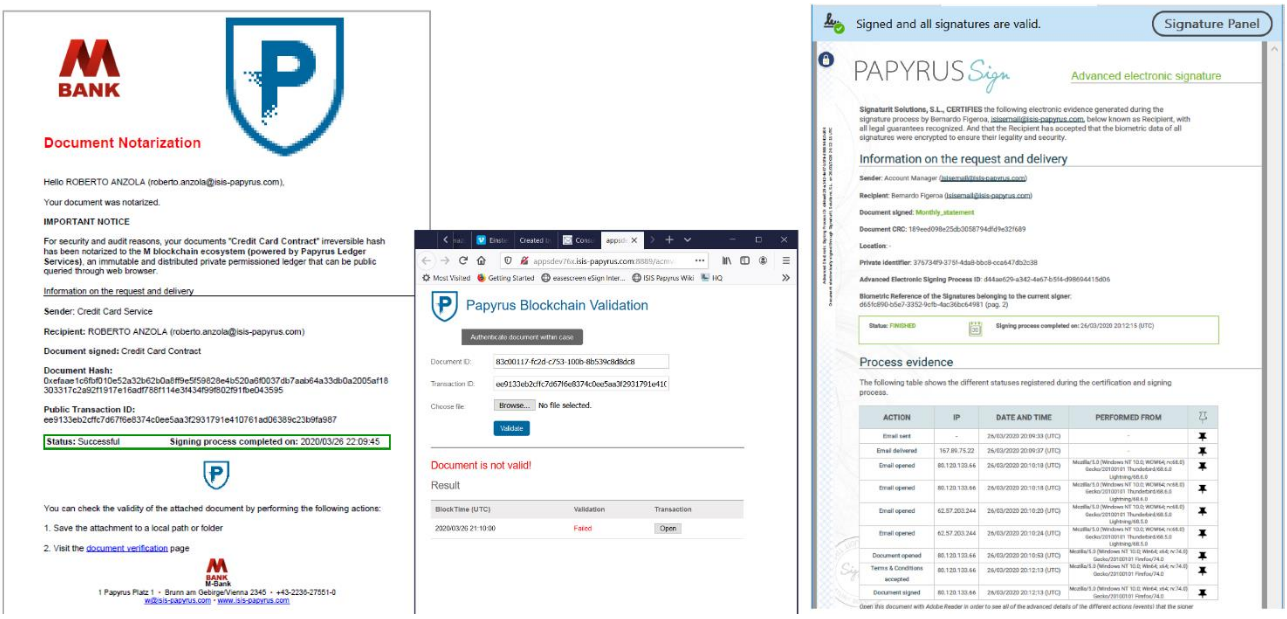
- all data encrypted, ensuring they can only be read and signed by designated users

Signee consent for the capturing of both his/her personal and biometric data

5.5 Auditing

Papyrus has extensive tracking, tracing, monitoring and auditing capabilities, covering the complete life-cycle of documents and all objects in the system with a full information on who has accessed each resource, when and why.

The auditing documentation produced by The Papyrus Sign solution fill the requirements from eIdas, ESIGN and UETA regulations standards covering EU and US.



Document Notarization

Hello ROBERTO ANZOLA (roberto.anzola@isis-papyrus.com),

Your document was notarized.

IMPORTANT NOTICE

For security and audit reasons, your documents **"Credit Card Contract"** irreversible hash has been notarized to the **M blockchain ecosystem (powered by Papyrus Ledger Services)**, an immutable and distributed private permissioned ledger that can be public queried through web browser.

Information on the request and delivery

Sender: Credit Card Service

Recipient: ROBERTO ANZOLA (roberto.anzola@isis-papyrus.com)

Document signed: Credit Card Contract

Document Hash:
0xefaae1c6fbf010e52a32b62b0a8ff9e5f59828e4b520a6f0037db7aab64a33db0a2005af18303317c2a92f1917e16adf788f114e3f434f99f802f91fbe043595

Public Transaction ID:
ee9133eb2cffc7d67f6e8374c0ee5aa3f2931791e410761ad06389c23b9fa987

Status: Successful **Signing process completed on:** 2020/03/26 22:09:45

You can check the validity of the attached document by performing the following actions:

1. Save the attachment to a local path or folder
2. Visit the document verification page

M-Bank
1 Papyrus Platz 1 • Brunn am Gebirge/Vienna 2345 • +43-2236-27551-0
w@isis-papyrus.com • www.isis-papyrus.com

appsdev76x.isis-papyrus.com:8889/acm

Papyrus Blockchain Validation

Authenticate document within case

Document ID: 83c00117-fc2d-c753-100b-8b539c8d8dc8

Transaction ID: ee9133eb2cffc7d67f6e8374c0ee5aa3f2931791e41(

Choose file: Browse... No file selected.

Validate

Document is not valid!

Result

BlockTime (UTC)	Validation	Transaction
2020/03/26 21:10:00	Failed	Open

Signed and all signatures are valid.

Signature Panel

PAPYRUS Sign

Advanced electronic signature

Signaturit Solutions, S.L., CERTIFIES the following electronic evidence generated during the signature process by Bernardo Figeroa, isisemail@isis-papyrus.com, below known as Recipient, with all legal guarantees recognized. And that the Recipient has accepted that the biometric data of all signatures were encrypted to ensure their legality and security.

Information on the request and delivery

Sender: Account Manager (isisemail@isis-papyrus.com)

Recipient: Bernardo Figeroa (isisemail@isis-papyrus.com)

Document signed: Monthly_statement

Document CRC: 189eed098e25db3058794dfd9e32f689

Location: -

Private identifier: 376734f9-375f-4da8-bbc8-cca647db2c38

Advanced Electronic Signing Process ID: d44ae629-a342-4e67-b5f4-d98694415d06

Biometric Reference of the Signatures belonging to the current signer:
d65fc890-b5e7-3352-9cfb-4ac36bc64981 (pag. 2)

Status: FINISHED **Signing process completed on**: 26/03/2020 20:12:15 (UTC)

Process evidence

The following table shows the different statuses registered during the certification and signing process.

ACTION	IP	DATE AND TIME	PERFORMED FROM	
Email sent	-	26/03/2020 20:09:33 (UTC)	-	
Email delivered	167.89.75.22	26/03/2020 20:09:37 (UTC)	-	
Email opened	80.120.133.66	26/03/2020 20:10:18 (UTC)	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101 Thunderbird/68.6.0 Lightning/68.6.0	
Email opened	80.120.133.66	26/03/2020 20:10:18 (UTC)	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101 Thunderbird/68.6.0 Lightning/68.6.0	
Email opened	62.57.203.244	26/03/2020 20:10:20 (UTC)	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101 Thunderbird/68.5.0 Lightning/68.5.0	
Email opened	62.57.203.244	26/03/2020 20:10:24 (UTC)	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101 Thunderbird/68.5.0 Lightning/68.5.0	
Document opened	80.120.133.66	26/03/2020 20:10:53 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0	
Terms & Conditions accepted	80.120.133.66	26/03/2020 20:12:13 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0	
Document signed	80.120.133.66	26/03/2020 20:12:13 (UTC)	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0	

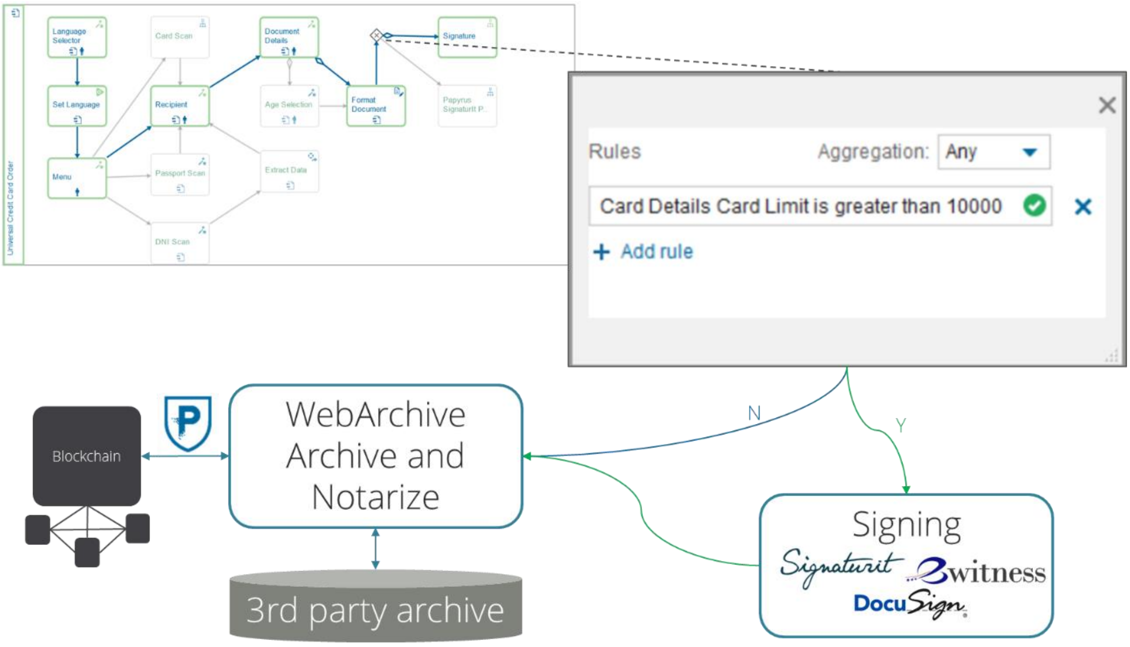
Open this document with Adobe Reader in order to see all of the advanced details of the different actions (events) that the signer

On top of the base auditing capabilities for all objects handled by the Papyrus Platform Notarization and and an signed auditing document containing all details regarding the signature process is provided.

5.6 Cost optimization using Papyrus Sign Solution

Using the Papyrus platform combining Papyrus Sign and ACM gives an unique flexibility to optimize the cost of managing digital signatures by introduces intelligent business rules into the workflow which dynamically determines the level of signatures, notarization and auditing required for a specific document based on data or user selection.

Maybe the value of a contract needs to be above a certain value to justify the added cost of signing the document with an authorized external signature authority such as SignaturIT, Docusign etc – while the lower value contracts are stored and notarized using only blockchain.



Rules

Aggregation: Any

Card Details Card Limit is greater than 10000

As another added value by the Papyrus platform process capabilities is that application of the Digital signature can be reserved for the final contract, while initial offers, interim versions, proposals etc. can be documented and stored for auditing purposes in blockchain – while only the final contract version is signed with a digital signature by involved parties by a thrusted external authority such as SignaturiT.

Signaturit services are part of the PapyrusSign solution and is a legally trusted solution integrated in the Papyrus platform.

6 Summary

More and more organizations are digitizing their paper processes and even documents with legal consequences are being processed increasingly often digitally such as contracts, mortgages and deeds. Digital signatures are an important element enabling business digitalization efforts, lowering cost and increase the easy of doing business both between companies (B2B) and between business and consumers (B2C).

As a result, the use of electronic signatures is rapidly on the rise and are in some countries and industries quickly becoming the norm instead of physical signatures.

7 Glossary

7.1 Terms

Hash	A hash value (hash for short) is a number which is calculated from any quantity of data such as documents, certificates, messages, etc. This number is often much shorter than the original data (approx. 20 bytes). The hash value has the characteristic that it is the same for the same data and is almost certainly unique for different data. The original data can also not be determined from the hash value. For the calculation hash algorithms are used such as SHA-1 or SHA-2.
Key	The certificate contains a public key which is used to verify the signature. The public key has to match a private key which is used to create the signature and has to be kept in a safe location.
Token	A “container” (part of the HSM, USB stick, smartcard, etc.) which contains private keys and protects against unauthorised access. For practical reasons the token often also contains corresponding certificates and public keys which do not need to be protected.
Verification, verifying	A signature is verified as follows: the signature is extracted from the document and decrypted with the public key. From this comes the hash value of the data at the time of signature. Afterwards the hash value of the signed data is formed again and compared with the hash value from the signature. If the two values correspond, the data have not been changed and are trusted (integrity check). From the signature message the certificate can also be extracted and the signatory can therefore be identified (identity check). Other checks regarding certificate validity and the time stamp are possible depending on the type of signature.
Signature, signing	Data with which the integrity and authenticity of a document can be ensured. The signature is essentially made as follows: the hash value is formed from the data which is to be signed and this is encrypted with the private key. The signature is packed into a CMS message together with certificates and checking information and as an option is embedded in the signed document.
Certificate	A certificate is an electronic certification of the identity of a natural or legal person. The certificate also contains a public key for which the person possesses a corresponding private key. With this private key the person can generate digital signatures. Any person can verify this signature with the help of the certificate.
Encryption	Data are encrypted so that outsiders cannot deduce their meaning. For the communication between sender and recipient, the recipient generates a key pair consisting of a private and a public key. If the sender now encrypts the data with the public key, only the recipient can decrypt the data because the recipient remains the sole owner of the private key. For the encryption, algorithms like RSA with key lengths of currently 2048 bits are used. The usual procedures for digital signatures are based on this technology

7.2 Abbreviations

ACM	Adaptive Case Management (ACM) is a method for organizing and structuring work within an organization. It strives to avoid the limitations of rigid process management (i.e. BPM) and improves the lack of complexity of simple case management. It aims at better handling knowledge work, which is loosely structured and unpredictable work that cannot be properly modeled with strict process management rules. Typical knowledge work

	includes strategic planning, customer service (insurance claims, social security), legal, investigative and analytical work, patient care and many technical projects.
ASN.1	Abstract Syntax Notation #1: Description language for the syntax of digital messages. For the binary encoding of the messages suitable standards are used here (e. g. X.690).
BER	Basic Encoding Rules: Easy to handle rules for the binary encoding of digital messages.
CA	Certification Authority: Accredited issuer of certificates. Digital signatures rely on public and private keys. Those keys have to be protected in order to ensure safety and to avoid forgery or malicious use. When you send or sign a document, you need assurance that the documents and the keys are created securely and that they are using valid keys. CAs, a type of Trust Service Provider, are third-party organizations that have been widely accepted as reliable for ensuring key security and that can provide the necessary digital certificates. Both the entity sending the document and the recipient signing it must agree to use a given CA.
CAdES	CMS Advanced Electronic Signatures: An ETSI Standard for the standardisation of CMS-based digital signatures.
CMS	Cryptographic Message Syntax: Message format for digital signatures based on the ASN.1 syntax (also often called PKCS#7).
CRL	Certificate Revocation List: List of revoked certificates published by the issuer.
DER	Distinguished Encoding Rules: Rules for the binary and unique encoding of digital messages based on BER.
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport: An international standard covering different sectors for the exchange of electronic data in business transactions.
EFD	Swiss Federal Department of Finance: The Swiss authority informs about structure, tasks and about current financial administration themes.
ETSI	European Telecommunications Standards Institute: European organisation for the standardisation of digital signatures etc.
HSM	Hardware Security Module: Device for securely saving private keys and also for encryption and decryption.
ISO	International Standards Organisation: International organisation for the standardisation of PDF and PDF/A, etc. Switzerland is represented in the ISO by the Swiss Standards Body (SNV).
LTV	Long-Term Validation: Enhancement of digital signatures with additional data so that long-term verifiability is possible without online services. The additional data consist of the trust chain of the certificates from the owner certificate up to the root certificate of the issuer and also information which certifies the validity of the certificates at the time of signature.
OASIS/DSS	Organization for the Advancement of Structured Information Standards / Digital Signing Services: A standard of the OASIS organisation for signing services based on the XML syntax.
OCSP	Online Certificate Status Protocol: Protocol for the online query of the validity status of a specific certificate based on the ASN.1 syntax.
PAdES	PDF Advanced Electronic Signature Profiles: An ETSI Standard for the structure of CMS signatures and their embedding in PDF documents.

PDF	Portable Document Format: A file format standardised by ISO (ISO-32000) for document exchange. For frequent PDF applications there are special sub-standards such as PDF/A (ISO-19005) for archiving digital documents.
PIN	Personal Identification Number: Secret code needed for access to a token.
PKCS	Public Key Cryptography Standards: A series of proprietary standards of RSA Security Incorporated. The most common standards are: encryption of signatures (PKCS#1), message format for signatures (PKCS#7), interface to token (PKCS#11) and file format for keys and certificates (PKCS#12).
QES	Qualified Electronic Signature.
TLS	Transport Layer Security: Further development of Secure Sockets Layer (SSL), a hybrid encryption protocol for secure data transmission on the internet.
TSA	Time Stamp Authority: Accredited provider of time stamp services.
TSP	Time Stamp Protocol: Protocol for the online retrieval of cryptographic time stamps based on the ASN.1 syntax.
XAdES	XML Advanced Electronic Signatures: An ETSI Standard for the creation of signatures and their embedding in XML data.
XML	Extensible Markup Language: Format for the exchange of hierarchically structured data in text form between machines.
X.509	ITU-T Standard for a public key infrastructure to create digital certificates based on the ASN.1 syntax.
X.690	ITU-T Standard for encoding digital messages based on the ASN.1 syntax: Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).