trustseed

WHITE PAPER

GLOBAL SECURITY SOLUTIONS FOR THE DIGITAL ECONOMY

Reference to General Data Protection Regulation (GDPR)

and Digital Signature Management (e.IDAS)

2019

Communication to ITSOC

International Two-dimensional Code Industry Development Summit Organizing Committee

国际二维码产业发展峰会组委会

Doctor Eric Blot-Lefevre

Seal Of Excellence -European Commission -Commissioner for Regional Policy Corina Creţu and Commissioner for Research, Science and Innovation Carlos Moedas- *digitally registered by the European Commission Date: 2016.02.01 17:45:35 CET).*

TrustSeed SAS Capital € 5.450.000 Office : 49 Bis Avenue Franklin-D-Roosevelt, 75008, PARIS – France
Dc. E. Blot-Lefevre -Chairman – ebl@trustseed.com – 33.607343163.

Preamble

Eric Blot-Lefevre, PhD in Economics and Cybernetics, has developed the first treasury software and financial instruments, in addition to his functions as treasury director for the L'Oréal, Thomson and Crédit Lyonnais Capital Markets groups. He was CEO of the Concept and XRT IT Groups sold to SAGE, and Hyperion (IMRS) sold to SAP.

He was a shareholder and a director of FININFO https://fr.wikipedia.org/wiki/Fininfo. He was then Central Director of the Crédit Lyonnais Group in charge of restructuring the Group (Accounting and IT Capital Markets), the financial security of the CDR (Defeasance), and the restructuring of the Stock Market (creation of Euronext by SICOVAM of which he becomes administrator).

In 1998, he became President of the European Federation of EDI Associations, ECE, Electronic Commerce Europe, sponsored by the European Commission. With the President of the Thales Group, Alain Gomez, he created the company Cashware, the first company to develop a civil signature “Offline” with the 1999 European Directive. It was associated with the American start-up Valicert, whose mission was to aggregate lists revocation of certificates from different CA’s (IDENTRUST).

In the year 2000, Chief Executive Officer of XRT, he launched Kyriba.com, a start-up that aims to provide financial management with cash management and financial instruments in SaaS, including an "off-line" electronic signature compliant with transfer security.

In 2002, TrustSeed SAS was created to develop the research and development of advanced “On-line” signatures, in cloud computing, in order to facilitate users a multilateral signature, visible and always verifiable. Eric Blot-Lefevre will participate between 2008 and 2017 in the main working groups of the European Commission for the preparation of the e.IDAS Regulation regarding qualified or advanced signature, and for the preparation of the regulation of Personal Data Protection (GDPR). He participates in the DG Connect Working Group (SSEDIC, NIS Platform, SRA Strategic Research Agenda) and in the work of “Trust in Digital Life” TDL Association (https://trustindigitallife.eu/) and Forum Atena France. Several publications concerning the 3DSA standard are available on the ENISA website https://resilience.enisa.europa.eu/nis-platform/WG1/shared-documents;

TrustSeed SAS will be awarded to the European Commission (Commissioner for Regional Policy Corina Creţu and the Commissioner for Research, Science and Innovation Carlos Moedas, Seal of Excellence, digitally registered by the European Commission Date: 2016.02.01 17:45:35 CET):
Seal of excellence "for its security and trust architecture built on a trinary mode with an advanced signature, visible, verifiable and certified by an independent validation instance”.

Trustseed also wins an award from the TDL Association by signing in a certified digital identity certificate in SaaS (Azure) and Cloud Computing (Trinary architecture), in partnership with Microsoft Azure.

The first client of TrustSeed is SAP to mass deploy different modes of signatures "Penseal" respecting the obligations of the aforementioned Regulations. More than 11 patent families representing 200 national patents have been deployed since 2010 on topics relating to trinary networks, advanced signatures, collaborative encryption modes and digital unique file issuance for transferable accounting and financial values.

To facilitate the understanding of the "Penseal ©" signatures used by Companies thanks to the technical means of their Subcontractors, the Qualified Operators (electronic stamp, time stamp, encryption), the white paper explains the regulatory provisions and the solutions implemented to make the Exchange Management easier, safer and less expensive.

With Valesign ©, Eric Blot-Lefevre is preparing a new generation of platforms adapted to the needs of States and Large Communities, for the application of their digital codes of conduct, for their intercommunity exchanges, and for international data transfers (Commerce, Bank and Insurance).

trustseed

CHAPTER 1 :

THE GDPR REGULATION and THE WORLD MARKET

CHAPTER 2 :

THE GDPR REGULATION AND ITS STRATEGIC OBJECTIVES

CHAPTER 3 :

COMPLIANCE OF 20 INTERNAL SECURITY SOFTWARE FOR COMPANIES

CHAPTER 4:

QUALIFICATION CRITERIA, CERTIFICATION CRITERIA, GDPR APPROPRIATE GUARANTEES

General conclusion

In the near future, the selection of competent market players in digital exchanges will be based on certification criteria for security software, and on the legal qualification of trusted services, responsible for processing, and capable of applying digital codes of conduct .

This draconian selection at the global level is the price to pay to protect Consumers and States increasingly exposed to uncontrolled risks. This is the price to pay to reduce the economic risks that the States always learn at their expense the cost of the bill and the social fracture.

These digital exchanges, which are progressing considerably, will be controlled by a few key players (fewer than perhaps the number of Countries in the world), and more than 30% of the volume of these exchanges will be cross-border and controlled at long distance.

In these conditions, we understand the challenge of e-commerce and digital finance whose means of regulation and resilience must necessarily develop prevention in all ecosystems and between Communities and responsible Nations.

In this evolution that gives a premium to qualified Operators, able to overcome technological barriers, a new passport for commercial and financial intermediation is emerging which will no longer be given to everyone, and without severe financial conditions.

trustseed

CHAPTER 1 :

THE GDPR REGULATION and THE WORLD MARKET

Growth of e-commerce

According to the WTO, global e-commerce accounted for a total of US $ 27.7 trillion in 2016, up from US $ 19.3 trillion in 2012.

B2B e-commerce is 6 times larger than e-commerce between Business and Consumer (B2C) WTO Report Page 21 https://www.wto.org/english/res_e/statis_e/wts2018_e/wts2018_e.pdf.

Global sales of BtoC e-commerce totaled $ 2,304 billion in 2017, up 24.8% from 2016, according to eMarketer. Online sales now account for 10.2% of total retail sales worldwide, up from 8.6% in 2016 and 7.4% in 2015.

Growth in the dematerialization of accounting, administrative and financial documents

Economic analysis of a region like Europe:

The sum of the economies of the 28 EU Member States corresponded to a GDP of EUR 15 330 billion in 2017. In comparison, global GDP was estimated at that date at around EUR 70 000 billion (Source: the International Monetary Fund).

Global GDP is therefore 5 times higher than European GDP).
https://www.touteleurope.eu/actualite/le-pib-des-pays-de-l-ue.html

According to the statistics mentioned by the SSEDIC Working Group, Scooping Single European Digital Identity Community, published in DG Connect (European Commission) in 2017 and published on the website of the European Network Information Security Agency ENISA- (https://resilience.enisa.europa.eu/nis-platform/WG1), the total value of services and transactions (Trade) in Europe is equal to € 50.000 billion, or 3.26 times the value of European GDP. The number of documents recorded is 240 billion €, and the average monetary value per document is 208 €.

http://www.trustseed.com/index.php/en/context

The number of payments in Europe is 20 billion (2.5 times less than the number of services and transactions) and the number of financial instruments in the Capital Markets another 20 billion.

The European Commission estimated in 2014 that the dematerialization (legal digital transformation) was to reduce by 70% the current cost of the documentary management evaluated by the European Commission to 1.000 billion euros, in particular with a saving of 243 billion € on invoices .

The unit cost of hybrid management (Paper and Electronic-File) is 4.17 € per document. This price concerns the incoming (Customer) and outgoing (Supplier) management of 240 billion accounting documents: this price should fall to 1.25 € with the reduction of costs, deadlines and risks https://ec.europa.eu / growth / content / final-report-expert-group-e-invoicing en

But in addition to the cost of physical, manual and visual treatment, one must add the additional cost of errors, malfunctions, and frauds. For example, PWC estimates that 7.5% of paper documents are lost or misclassified.

https://economia.icaew.com/features/july-2014/paper-weight#sthash.PgzTiBsa.dpuf

Internal frauds or "connivance" or "complicity" between employees hired by companies are growing faster than the damage of cyberattacks.

Management Software Editors whose business is to apply codes of professional conduct and accounting plans do not know how to defend companies against all forms of fraud invented in the cloud and within companies:

• Falsification of document, False authentic document, falsification of the uniqueness of the document

• Backdated document,

•Identity theft,

• Wrong in signing , in writing and up-dating

• Non-compliance of mandatory legal content,

• Violation or misuse of procedures,

• Breach of trust

• Destruction of evidence

• Break in traceability (link between management operations)

• Breakdown of pairing (link between Identity, attributes, proxy and permission)

• Breakdown of matching (link between two commercial or financial documents)

• Computer intrusion, viruses, spam, organised outside Attack etc.

• Failure confidentiality (indiscretion)

• Abuse of rights or power

• Theft of secrets, codes, attributes, data information or ownership (IP)

• Forfeiture or hijacking of signature keys and encryption keys.

• Forgery in violation of obligations of separation between legal responsibilities

An article by GEOS in Great Britain titled "Theft of data in vogue in the United Kingdom" indicates that one in three senior executives steals data from his company. In 48% of cases, these data relate to methods, procedures and industrial property; and in 14% of the cases, the theft concerns confidential financial data.

The European Commission estimates tax frauds exceeding 1000 billion a year. https://ec.europa.eu/taxation_customs/fight-against-tax-fraud-tax-evasion/a-huge-problem_en

A recent study confirms a tax invasion in Europe for the year 2018 of more than 850 million euros . https://www.humanite.fr/evasion-fiscale-825-millions-manquent-europe-667176 (Richard Murphy-University of London).

The falsification of documents is another steadily increasing scourge that leads holders of fraudulent documents to lose out, sooner or later, huge amounts of money; the SNT University of Luxembourg mentioned in 2017:

"Current approaches to managing digital assets are far-reaching because they are prone to errors and faults that are very late. Only in 2012, the Italian police seized $ 6 trillion of dummy US bonds, which is an indicator of the gaps in this area. "

Regarding the 20 billion payments made in Europe, for a value of € 2500 per regulation on average, fraud is also constantly increasing.

For example, the Banque de France's Observatory of Payment Security confirms that check fraud has risen sharply in 2018, from 52% / year in one year to 450 million euros. https://www.latribune.fr/entreprises-finance/banques-finance/flambee-de-la-fraude-au-cheque-attention-aux-nouvelles-escroqueries-en-ligne-alerte-la-banque-de- France-823102.html

More than 1.2 million households reported being victims of at least one bank scam in France in 2016, more than doubling in six years (500,000 households in 2010) and causing an average monetary loss of 300 € per person stolen. https://www.latribune.fr/entreprises-finance/banques-finance/fraudes-bancaires-1-2-million-de-menages-touches-778652.html

For the countries of the European Union, 512 million inhabitants, the theft on means of payment represents a cost of the order of 3 billion € per year.

The annual cybercrime represents € 600 billion worldwide, that is to say a levy of 14% on the Internet activity of 2016: https://www.mcafee.com/enterprise/en-us/assets/executive -summaries / es-economic-impact-cybercrime.pdf

All errors, illegalities, falsifications, frauds and indiscretions committed in Europe on services, transactions, industrial property, payments and financial instruments (Capital Markets) represent at least, with tax invasions, an additional cost for € 1,300 billion documentary exchanges.

The current unit documentary cost of 4.17 €, with this collateral damage, increases and it is of the order of 8, 34 € by document.

The fight against fraud imposes in the GDPR Regulation to the “Trust Services” and their “Subcontractors” systematic prevention against errors and fraud. This heavy legal obligation which weighs on the Managers of the Treatment (Art.24), that is to say on the Services of trust (Front Office) will contribute to the reduction of the risks and delays of digital processing (real time) on documents created, signed, encrypted, sent and transferred.

In conclusion, in the European Gross Domestic Product, which is 15,330 billion euros, documentary dematerialization will reduce the costs of documentary exchanges by 700 billion euros, and prevention documentary fraud will reduce damage collateral of € 1,300 billion.

The RGPD Regulation imposes on-line service providers the lawfulness, loyalty, transparency and prevention of fraud (Ali.46).

The total economic improvement organized by the RGPD Regulation is € 2,000 billion per year in Europe for Gross Domestic Product of € 15,330 million, a relative increase of 13%.

We can also say that the European Gross Domestic Product 15.330 billion euros is burdened or degraded by 13% representing 2,000 billion euros of invisible levies and detrimental to the economy and competitiveness. This 13% leakage rate in Europe's resources must be compared to the average net profit of companies which is less than 5% per year.

If the total financial value € 50,000 billion is exchanged in Europe for a gross domestic product of € 15,330 billion (coefficient 3.26), we deduce that for the global GDP $ 84 740 billion, (https://fr.wikipedia.org / wiki /), the whole Countries List regarding nominal Gross Domestic product is 75,000 billion €, and the value of the exchanges is of the order of 244 500 billion euros.

And for this value of global consolidated trade, with an average financial value per document of € 208, we obtain a number of documents equal to 1,175 billion.

At 1.25 € the price invoiced for the digital transformation of a management file into an original, signed, encrypted and tamper-proof documentary file, the global turnover of "intra-day" accounting dematerialization is 1,469 billion €

Assuming a weighting of the estimate of the number of documents to account for a lower proportion of documents in developing Countries, weighting by 50%, the volume of documents is 734 billion per year in the world.

By assuming a 50% reduction in the digital documentary unit price, which consequently improves the competitiveness of the companies, the initial price of € 1,25 will stabilize at € 0,62 or $ 0,75.

The reduction is justified to the extent that 60% of the documents have only one signature, 30% has 2 (Acknowledgment of receipt, Contract) and 10% a number of signatures greater than 2. And this is the latter type documentary topology that costs the most.

The turnover corrected by these adjustments (Volume and price) is:

750 billion. € 0.62 = € 465 billion turnover per year worldwide.

	€ Milliards Europe	€ Milliards Monde
Gross domestic product	15 330	75 000
Value of Exchanges	50 000	**244 500**
Volume of documents	*240*	1 175
€ Value per document	208	208
Unit cost of management	4.17 €	4.17 €
Cost reduction	70 %	70 %
Original Digital Cost	1.25 €	1.25 €
Digital market value	300	1469
Weighting Price 2024	0.62 €	0.62 €
€ Market Weighted Value Turn over	149	
Weighted Documentary Volume		588
€ Weighted Value Market		365
Number of payments	*20*	98
Amount Payment Medium	2500 €	2495 €
Number of enterprises	20.000.000	60.000.000

Statistiques OMC -EC.SSEDIC DG Connect– NIS https://resilience.enisa.europa.eu/nis-platform/WG1),	€ Billion World	€ Billion China
Gross domestic product	75 000	13 000
€ Value of Exchanges	**244 500**	42 400
Volume of documents	1 175	203
€ Average value per document		
Unit cost of management	4 .17 €	
Cost reduction	70 %	
Unit cost of Original Digital Uniqueness Creation	1.25 €	
€ Digital Market Value in Europe (28 States)		
Weighting Price	0.62 €	Digital Policy
€ Weighted Value Market Europe (Turn over)		
World Weighted Document Volume	588	
€ Weighted Value Market World -50 %	€ 365	
Number of payments	98	
Average Amount Payment	€ 2495	

trustseed

CHAPTER 2 :

THE GDPR REGULATION AND ITS STRATEGIC OBJECTIVES

The EU regulation 910/2014 on online signing, mentioned in 2014, before the RGPD 2017 regulation, that "Consumers, companies and public authorities do not trust, especially because of a sense of 'Online Legal Insecurity'. "

"Indeed, the previous Directive 1999 / 93.CE on the electronic signature (1999) governed electronic signatures without providing a complete cross-border and cross-sectoral framework for secure, reliable and easy-to-use electronic transactions" (European Parliament)

To provide businesses and their customers with legal certainty online, the RGPD regulation first made provisions for each legal person or physical entity to be certain:

1. Identities of their counterparties
2. Rights ,Permission , Authorization of their counterparties
3. Contacts accepted by their counterparts with strong consent
4. Signature and encryption keys under their exclusive control
5. Uniqueness of originals of tamper-proof documents
6. Certification of integrity, timestamping and document traceability
7. The legal value of consent signatures, to be visible and verifiable
8. Confidentiality of signed data
9. Proofs of sending and receiving mail
10. Security of transfer of value or financial instrument
11. Means of rectification, erasure, opposition and portability
12. Pseudonymization and profiling means

GDPR Regulation establish appropriate certification standards and safeguards for the protection of users

To achieve a climate of trust, the RGPD Regulation has established a division of competencies and responsibilities between:

1. An Online Provider responsible for "Trust Services" (Controller Art.24),

2. A Subcontractor Operator of Originals of Encrypted Documents, Signatures of Consent, Encrypted Communication (Documentary Correspondence) and Transfers (Financial instrument or Personal Assignments, any deed of title, patent or industrial property).

3. A Validation Body ensuring the online legal value of original documents and signatures, communication or transfer with all legal means of preservation, rectification, opposition, erasure or portability.

This qualified trinary network device implements in the RGPD regulation 20 important digital functions.

These functions, which we will enumerate, are subject to a preventive control of the identities, the rights, the permissions, the proxies and the consents, as well as an evaluation of the conformity of the operations of emission, integrity, timestamping , signature, encryption, transmission of documentary data or transfer of financial securities.

The RGPD also imposes on the part of intermediaries mandated in these functions, transparency, legality, loyalty and confidentiality measurable in real time so as to safeguard the interests of natural or legal persons, and in a way to demonstrate that their rights and their signature and encryption keys are still under their exclusive control.

Finally, the GDPR Regulation requires qualified intermediaries to carry out data transfers in such a way that each person may, on the data transferred to his account, and on data subsequently transferred to a counterparty's account, benefit from the same persistent rights (rectification, deletion, opposition, portability, ...).

The technical and operational means must be maintained and persistent by always providing the same appropriate guarantees (identification, authentication, sealing, signature and encryption).

Rights validation and conformity verification mechanisms must still work for subsequent third-party communication or transfer, so as to sustainably preserve an extended environment of trust between the two or many Parties.

To comply with the chain of validation extended to the many individual or collective rights imposed by the GDPR Regulation, by maintaining the revocation lists between interchange conventions or established contacts, and to comply with the extended conformity control mechanisms on all documentary operations subject to professional codes of conduct, the RGPD regulation has introduced several legal solutions.

The first solution is qualified by the Certification Authorities in their business and in their functional scope: Certificates of identity, integrity and timestamp.

The second solution is "advanced" by documentary providers to deliver "appropriate safeguards" Art 41-46 from "appropriate technical and organizational means" Art 27. The periodic evaluation of the conformity of "advanced solutions" by " technical and organizational means ", as well as by" impact analyzes "Art.35, allows trust services, and subcontractors operators, to obtain" by design "certifications whose control mechanisms Art.41 activate a complete set of revocation lists followed by an independent validation instance.

In this way, all personal services in terms of proxy management, contacts, mandates (SLAs), and signing and encryption keys can operate in real time with the corresponding revocation lists, and they can work in interoperability with all the other services and operators listed and used by counterparties.

In this way, all human rights (Data Protection, Strong Consent, Correction, Deletion, Opposition, Pseudonymisation, Portability, Transfer ...) are respected in accordance with the GDPR Regulation.

Both "qualified" and "advanced" solutions can be mixed in order to take advantage of the qualification of the Certification Authorities, especially for the certificates of identity, authentication, sealing and time stamping.

The combination of qualified and advanced solutions then makes it possible to take advantage of the flexibility of the advanced solutions "by design" which cover, with the "appropriate guarantees" the whole spectrum of the management of the personal rights articulated around the proxies, the permissions, the contacts, the consents, the signatures and encryption, between several signatories affiliated to different trust services.

The advanced solution solves the problems of interoperability between the controllers (Trust Services Art.24), the subcontractors (operators Art.28) and the validation instances (Control Art 40 - 41).

The separation of the responsibilities of the trusted third parties in mandatory to guarantee the protection of the data and the keys of signature and encryption, and the treatments corresponding to them.

Article 28 :Subcontractor

Where a processing operation is to be carried out on behalf of a “Data Controller”, the “data controller” shall use only “subcontractors” who provide sufficient assurance that the 'appropriate technical and organizational measures' in such a way that the processing meets the requirements of this Regulation and guarantees the protection of the rights of the data subject.

The subcontractor process personal data only on the basis of documented instructions by the controller, including with regard to transfers of personal data .

Depending on the choice of the data controller, the subcontractor deletes all personal data or sends them back to the data controller upon completion of processing services and destroys existing copies.

Without prejudice to Articles 82, 83 and 84, if, in breach of this Regulation, a subcontractor determines the purposes and the means of the processing, he shall be considered in breach by acting wrongly as a controller in respect of that treatment.

Article 29

Processing carried out under the authority of the Controller by the Subcontractor

The Subcontractor and any person acting under the authority of the Controller, who has access to personal data, may not process such data, except at the direction of the controller.

Article 82

Right to reparation and liability

1. Anyone who has suffered material or moral injury as a result of a breach of this Regulation shall have the right to obtain from the controller or the processor compensation for the damage suffered.

2. Any Controller who has participated in the processing is liable for the damage caused by the processing which constitutes a violation of this Regulation. A Subcontractor shall be held liable for the damage caused by the processing only if he has not complied with the obligations laid down in this Regulation which are specifically incumbent on the subcontractors or he has acted outside the instructions lawful or unlike the Controller.

Regarding the protection of personal data with signature or encryption keys, Article 26 e.IDAS Regulation sets out the requirements for an advanced electronic signature:

The advanced electronic signature must:

(a) be uniquely linked to the signatory;

(b) identify the signatory;

(c) have been created using electronic signature creation data that the signatory may, with a certain or high degree of confidence, use under his exclusive control; and

d) be linked to the data associated with this signature so that any subsequent changes to the data are detectable.

In the subject 51, e.IDAS Regulation says :

The signatory must be able to entrust the electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has exclusive control over the use of his data. electronic signature creation, and that the use of the device meets the requirements for a qualified electronic signature.

In these draconian conditions of key protection, it is necessary to distinguish three levels of key management corresponding to the legal separation of skills between the three trusted third parties "Controller", "Sub Contractor - Processor" and Control-Validation body.

1. The functions of activation and revocation of the keys associated with the digital identity and the attributes of trust of the person (signatory), and possibly associated with those of his client (Account's Holder) if he is authorized: this is the mission of the Controller (Art.24) .

2. Personal key applications related directly or indirectly to documents and procedures necessary for integrity management, timestamping and strong personal consent. This is the mission of the subcontractor (Art.28)qualified in terms of signature processing.

3. Protection of personal keys held in a special secure area (Key Vault), protected by a Revocation List and administered by a Control-Validation instance (Art.40.41)that records the uses.

To complete this analysis of the security of the signing keys, it is useful to mention the opinion of the legislator who recognizes that it is necessary to innovate informally to achieve the results indicated in the regulation.

(Alinea 55) An IT security certification based on international standards, such as ISO 15408 and related assessment methods and mutual recognition agreements, is an important tool for verifying the security of signature creation devices qualified electronics and should be encouraged.

However, innovative solutions and services, such as mobile signature and cloud-based signing, require a "technical and organizational solution" for qualified electronic signature creation devices for which security standards may not yet exist or for which the first computer security certification is under review.

The security level of these qualified electronic signature creation devices could only be evaluated using other processes when these security standards do not exist or when the first computer security certification is under consideration.

Punishments

The obligations relating to the regulation RGPD and concerning the rights of the people and the obligations relating to the Services of confidence, are sanctioned in case of default by fines of up to 4% of the turnover, and by a prohibition to treat online digital exchanges. (Disqualification of Trusted Online Services, or their Operator Subcontractor).

Article 83

General conditions for imposing administrative fines

1. Each Supervisory Authority shall ensure that the administrative fines imposed under this Article for violations of this Regulation

3. If a Controller or a Subcontractor deliberately or negligently breachs several provisions of this Regulation, in the context of the same processing operation or related processing operations, the total amount of the administrative fine may not be-not exceed the amount fixed for the most serious violation.

4. In accordance with paragraph 2, violations of the following provisions shall be subject to administrative fines of up to EUR 10 000 000 or, in the case of an undertaking, up to 2% of the total annual global business of the previous financial year, whichever is higher.

To comply with all these constraints, mainly 20 functions must be adapted to the obligations to satisfy the legal and IT security levels implemented in the inter-company communication networks:

1. The Certification of Identities in the trinary system (Art.28-42- e.IDAS Art.7) by the qualification of the Trusted Third Parties or the certification of means with "appropriate guarantees" (Art.42)

2. The means of authentication in the trinary system (e.IDAS Art.6-7-8) by the qualification of the provider with the "appropriate guarantees" (Art.42)

3. The Update of unambiguous personal rights (Art.35): Access (Art.15-32), Correction (Art.14), Revocation (Art.16-e.IDAS 24), Cancellation (Art.17 Right to forgetting), Opposition (Art.21),Pseudonymisation, Profiling (Art.4-13-22-47), Long-term preservation (Art.13-30), Portability (Art.20), Withdrawal of consent, Prevention against fraud (Art.47).

4. The Update of Digital Conventions: Powers, Permissions, Mandates, Signatories Contact Information.

Transparency and loyalty are principles of prevention against breach of trust concealed by opposing parties to a bilateral interchange agreement. Since Article 47 provides for the prevention of fraud against service providers, the invitation to consent without a contact (interchange agreement) must mention certain attributes or permissions the disclosure of which is mandatory in the codes of service providers professional driving.

This transparency makes it possible to avoid invitations with companies that are doubtful or disqualified for their bad behavior sanctioned by the national market authorities.

5. The Data Minimization (Art.25-47), Limitation (Art.18-19) and Purpose of Processing (Art.5-13-28-32).

6. The Long-term preservation of data, decryption and transmission to third parties by permutation of encryption keys.

7. The Transfer of ownership with appropriate guarantees (Binding Corporate Rules Art.47)

8. The exclusive control of the keys of the signature by consent and for the encryption, and the conservation of the proofs of validity of the signatures of consent, opposable with the thirds

9. The Certification in the Creation (Emission) and in the uniqueness of documentary Originals: unique data of creation (Art.25-28) ensured by the qualification of a provider or by the "appropriate guarantees" (Art.42) provided by "technical and organizational means"

10. The Certification of Integrity (Art 32.1) of Sealed Documents (Art.19-24-35 e.IDAS) through a qualified or organized provider with "appropriate safeguards" (Art.42) by the existing technical and organizational means in the trinary system

11. The Certification of sealed Timestamp (Art.19-24-35 e.IDAS) with the qualification of a provider or with the "appropriate guarantees" (Art.42) in the trinary system

12. The Certification of Traceability (Art.28-30) and Transparency (Art.12) Multilateral between Services and Subcontractors resulting from verification in a private and trinary blockchain (e.IDAS Art.28- 30-33) compliance constraints reviewed by a validation and control instance.

13. The Signature of Visible and Verifiable Consent without any risk of disclosure of the contents of the document to the outside (Annex II e.IDAS 1.a and d), and with the exclusive control by the signatory of his signature keys: key private and public key (e.IDAS -GDPR Art 28-42).

14. The signature of the notary or employee of the Visible and Verifiable Validation Body by demonstration after evaluation of conformity by control mechanisms (Art.40-41, E.IDAS Art.34)

15. The Protection of Personal Data from conception (Art.47), the default protection: encryption procedures (Art.32.1) in collaborative mode for all types of exchanges or transactions (Art.32.1)

16. The Secure correspondence between digital documentary accounts

17. The Interoperability Procedures (e.IDAS Art.7), Resilience (Art.32-47) and Commission rogatory (Corrective Measures Art 47.2.J)

18. The Dynamic rating of the Legal Value of Online Transactions (Art.47-e.IDAS Art.3-6)

19. The Evidence of operations: Treatment, (Art.4-30- e.IDAS Art.3-36), Confidentiality (Art.31), Transfer (Art.30-42), and Traceability (e.IDAS Art. 24). Matching identities, operations, and digital certificates.

20. The Follow-up of the Qualification of Third Parties of Trust or the monitoring of "Appropriate Guarantees" (Art.13-25-28) associated with "technical and organizational means" certified.

Under these conditions, all the current functions of "hash", "Sealed Hash" (Sealed Condensate), QR Code, and validation are to evolve in the private blockchain configured in the regulatory trinary system (Art.24-Art28 -Art40.41).

The digital functions governed by the e.IDAS and GDPR regulations are indicated as follows, depending on whether it is a model based essentially on "qualified solutions" by the certification authorities, or based on "advanced solutions". "by appropriate technical and organizational means" operating within the trinary framework of the RPGD Regulation (Art.24 / 28/40) with the" appropriate safeguards ".

trustseed

CHAPTER 3 :

COMPLIANCE OF 20 INTERNAL SECURITY SOFTWARE FOR COMPANIES

The need of the Digital Market : explanation of the problem

Professional management files are based on professional rules of the game. In particular, the mandatory information structures files to meet the constraints of each business and tax (Codes of Conduct GDPR Section 5 Art.40).

To transform a management document into a legal-financial-or-administrative document (Lawfulness), ensuring the full legal value of signatures and exchanges, enforceable against third parties, it is necessary to carry out 6 additional operations for each management document:

1.Guarantee the uniqueness and the integrity of the physical document and the timestamp (non-reproducible) realized in paper form or guarantee the uniqueness and the integrity of the documentary "file" and the timestamp with digital sealing or an electronic seal.

2. **Guarantee the authenticity and validity** (present value) of each identity, power and permission (or qualification) of the parties and signatories chosen (legal entities and natural persons), whether in paper form or in digital form.

3. **Guarantee,** with regard to their exchange agreement, **the accuracy of the correspondence** and **signature data**, in paper form or in electronic form, by checking the revocation lists which could invalidate each exchange or signatory.

4. **Guarantee the authenticity and validity of the signature manifested by consent**, either in paper form or in digital form, ensuring that the signature is **visible and verifiable at all times** by the signatory parties or by each authorized third party.

5. **Ensure that the physical or electronic means** for the transport of the document and signatures, are secured for both documentary correspondence and transfer of ownership.

6. Guarantee that each Issuer or Recipient may exercise his rights in a physical exchange or in a dematerialized exchange, using the functions of **withdrawal of consent**, **pseudonymisation**, **rectification**, **deletion, opposition and portability** of information to another trusted provider.

7. **Ensure that the confidentiality or documentary secrecy standards** are respected:

- or at the level of the separation of responsibilities between the trust service, the exclusive custodian of the personal data, and the "Subcontractor" with the limited number of data for a limited number of electronic operations :stamp and signature files.

-or at the level of confidentiality to encrypt personal data

-or at the level of protection of personal keys remaining at all times under the exclusive and demonstrated control of their owner.

In these circumstances, professional management software Publishers use digital processors and their subcontractors who are responsible for the creation of unique originals of documents and signatures, encryption, communication and transfer operations, including the control of an independent validation instance.

There are normally 20 security software programs that are organized differently depending on whether the current practice or the organizational mode of “Personal Data Protection” and the implementation of a visible, traceable and verifiable personal signature.

	20 Functions **Benchmark Score 1to 5**	Ternary Network- Advanced Solutions combining Qualified Certificates with « Appropriate Guarantees » by «Appropriate Technical and Organizational Means »	Usual Network Combining Qualified Certificates with low level of Appropriate Means
1	Identity	4	4
2	Authentication	4	4
3	Individual Rights Present value Updating	5	1
4	Interchange agreement Present value Updating	5	1
5	Minimisation/Limitation/Purposes of Data	4	2
6	Long-term storage of data	4	1
7	Property Transfer	5	1
8	Exclusive and enforceable control of keys	5	1
9	Certification of unique Originals of Document File	5	0
10	Qualified Certification of Integrity of Sealed Doc.	5	5
11	Qualified Certification of Timestamping	5	5
12	Certification of traceability and validation	5	1
13	Visible and Verifiable Consent of Digital Signature	5	0
14	Notary Employee Signature of Validation	5	0
15	Data Protection Encryption and Data Erasure	5	1
16	Secure Correspondence between Safe Digital Accounts	5	3
17	Interoperability Procedures, Resilience ,Letter of Request	4	1
18	Dynamic rating probative value of digital transaction	5	1
19	Digital proofs of operations	5	2
20	Follow-up of qualifications and appropriate safeguards	5	1
	TOTAL	95/100 95%	35/100 35%

trustseed

Comparison of the two models of security architecture and digital trust in their respective capacity to meet all the obligations of the GDPR Regulation and the NIS Network Information Security Directive implemented since 2017.

	20 Functions	Qualified Solutions CERTIFICATES EXISTING	Advanced Solutions CERTIFICATES + APPROPRIATE GUARANTEES
1	Identity	X	X
2	Authentification	X	X
3	Present value Personal Rights		X
4	Review Personal Agreements		X
5	Minimization/Limitation/Data Purposes		X
6	Long-term Preservation of Data	X	X
7	Transfer of ownership		X
8	Certification exclusive enforceable control of keys		X
9	Certification of unique originals		X
10	Certification of integrity by sealed document	X	X
11	Certification of timestamping	X	X
12	Certification of traceability and validation	Limited	X
13	Private Consent Signature visible and verifiable		X
14	Notary Validation Signature Visible and Verifiable		X
15	Protection and encryption of data (Safe Box)	Limited	X
16	Secure correspondence between digital accounts		X
17	Interoperability procedures, resilience, rogatory commission		X
18	Dynamic probative value of digital transaction		X
19	Digital Legal Proof of Operations and Delivery		X
20	Tracking of qualification Status and “Appropriate Guarantees”	Limited	X

trustseed

CHAPTER 4:

QUALIFICATION CRITERIA, CERTIFICATION CRITERIA, GDPR APPROPRIATE GUARANTEES

The separation between the Data Controller (Art.24) and the Subcontractor Operator (Art.28) is not only a legal reality (Rules mentioned in Chapter 2) but also practical, since each signature certification authority and electronic stamps, do not yet have "all the technical and organizational means" to manage end-to-end, multilaterally, on a cross-border basis, and in an instant interoperability, commitments by digital personal signatures.

To manage digital signature commitments end-to-end, it is necessary to comply with 42 legal obligations, of which we will list the articles of the GDPR and e.IDAS regulations.

By default, of a satisfactory overall solution, the controller will design, in addition to the qualified services provided by the certification authorities, appropriate technical and organizational means with the control mechanisms implemented or stipulated by the supervisory authority.

And the Code of Conduct Validation Authority (Art 40 GDPR) will provide the "appropriate guarantees" in addition to the certifications provided by the qualified Certification Authorities. These technical and organizational means must be periodically certified by certification bodies or by a Conformity Assessment Body.

The trusted third parties responsible for the processing (Trust Services Art.24) and their subcontractors (Operator-Processors Art.28) are submitted to operate in the digital market to a Qualification.

This qualification is a permission granted by the market control authorities responsible for enforcing the codes of conduct in each professional sector.

The qualification is already attributed to the Authorities of Certification which creates means of identification, sealing, signing, digital time stamping.

For other documentary intermediaries that offer a range of Services downstream of the identification, upstream or downstream of the sealing and signing operations, and in particular to reinforce the procedures of pseudonymisation, data limitation, power of attorney, contact (Interconnection Agreement), issuance (Original Documents), consent, encryption, communication, transfer and multilateral traceability between the parties, for example, it is necessary to design the “technical and organizational means” and to design the results control mechanisms, submitted to a validation body to deliver the "appropriate guarantees ”.

The validation instance organizes the checks in a private blockchain for which it has control of the verification criteria and of the revocation lists relating to the pseudonymisation, the protection of the personal codes and keys of signature and encryption, the management of the proxies, the inter-change agreements, and features related to mandatory security protection for future term transfers (Art.46 GDPR).

The technical and organizational means (Art.32) must be the subject of a data protection impact assessment, especially to preserve the rights relating to confidentiality, rectification, erasure, opposition, finalization of operations, and portability.

These rights must be exercisable in the context of the transfer of data between the parties concerned. The technical and organizational means are submitted to the Certification test so that trusted third parties can be qualified.

Software means certification is issued by conformity assessment bodies or certification bodies (Art.43 GDPR).

The 20 functionalities carrying out all the services provided to the users, natural person or legal person (employee), in their regulatory framework (Regulations e.IDAS 2014, GDPR 2017, and Directive NIS Network Information Security 2017) are treated in different ways according to the profession of each trusted third party, either qualified as a Certification Authority for certain areas of preference, or Qualified as Processing Manager (Art.24: Responsible of the Treatment- Controller) using the “technical and organizational means” of its subcontractors (Art.28) in all domains.

The control mechanisms established in Article 40.4 to assess in real time the validity of individual and social rights (Data Updated and Accurate: Art.5.1d), as well as to assess the conformity of operations performed by "technical and organizational means", they operate in a private blockchain dependent on the instance of validation.

It is therefore this validation body that keeps the exhaustive revocation lists and keeps the rights updated and their renewal at the expiry dates. It is thanks to this management of lists, deadlines and notations of digital identities that interoperability works instantaneously between the controllers and their subcontractors.

For example, three signatories (ID Certificates) on their behalf or on behalf of their companies of a document (Proxy), may be domiciled at three different trust services (a Post, a Bank, a Company), and these trusted services, responsible for processing for each user, may use different "subcontractors" to create the original documents, to seal and time stamp each original, to provide each signatory with a strong consent and legal signature interface, and to encrypt documents such that it is securely transmitted in the confidential accounts of the parties and subsequently readable by the authorized personnel, or transferable (original) or copiable (Duplicate) for the interest of another counterparty.

It is therefore useful to complete this white paper, to illustrate an example of distribution of functions between those who possess natively the certification obtained by certification authorities, and those who are obtained by “technical and organizational means” subject to the control of a independent validation body to provide users with "appropriate guarantees", including interoperability, and to safeguard their rights and personal data.

Finally, it is useful also for measuring the scope of responsibilities of the validation body, responsible for security, legal value, compliance (Codes of Conduct) and interoperability (Treatment Networks), to list the Identity Certificates Rating, the Authentication Means Notation, the revocation of rights, and the documentary services supervised by the validation authority or by more than one of them when there are several countries concerned or when there are several codes of conduct implemented.

Let's look at the Native / Additional Certification Scorecard (Software).

	20 Fonctions	Native Certification from Qualified Certification Authorities	Certification of « Appropriate Technical and Organizational Means" verified by Control Mechanisms from independent Validation Body (Appropriate Guarantees)
1	Identity certified		
2	Authentication certified		
3	Personal Rights updating		
4	Interchange agreement updating		
5	Minimisation/Limitation/Finalisation of Data Processing		
6	Long term Data Archiving		
7	Ownership Transfer		
8	Exclusive enforceable control of personal Keys		
9	Documentary Originals Uniqueness		
10	Documentary file sealed for Integrity Certified		
11	Timestamp file sealed for value date certified		
12	Traceability Conformity Control Mechanisms		
13	Mandatory Private Consent of signature visible and controllable		
14	Validation Employee Consent of Signature visible		
15	Data encryption and protection certified		
16	Document Accounts Correspondence		
17	Rogatory procedures, interoperability and resilience		
18	Probative value measurement of document signed		
19	Legal proof of operations and delivery		
20	Qualified Bodies Status List and Appropriate Guarantees List		
	TOTAL		

With regard to the responsibilities of the control and validation body, these concern the notation and certification of identities and software means, instant revocation lists of certain means and functions (authentication, payment), rights, credentials, permissions, agreements and signing or encryption keys.

The control mechanisms also make it possible to check the qualification of the numerous trust services, subcontractors operators, as well as the validity of the certificate of their signature keys. These mechanisms also make it possible to set compliance control criteria for each type of signature commitment (s).

trustseed

Here is the list of 24 security softwares from which the 42 obligations mentioned in the two GDPR and e.IDAS Regulations that we are going to inventory are most easily applied.

24 DIGITAL SOFTWARES

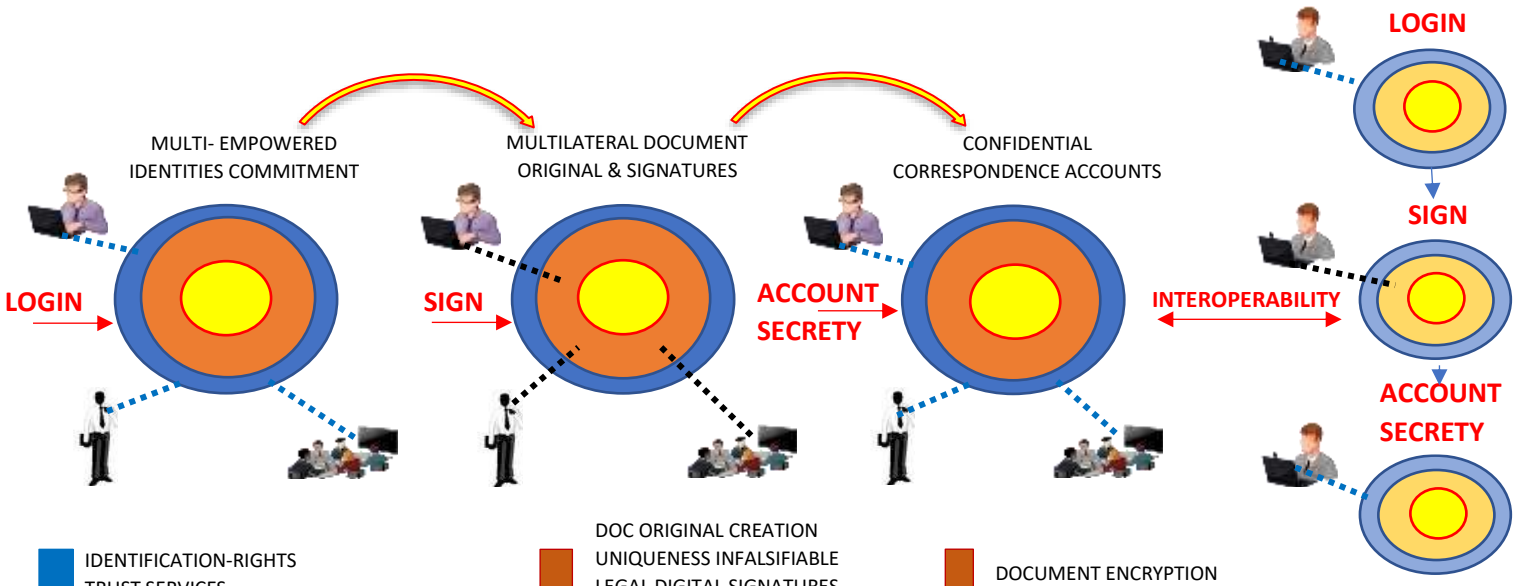
	Digital softwares list: Responsible of Treatment
1	Identity Management
2	Authentication Management
3	Individual Entitlements & Permissions
4	Documentary Commitment by Signatures
5	Interchange Agreement
6	Data Minimisation/Limitation/Purposes
7	Data Long-term Conservation
8	Rights Pseud.,Rectification, Erasure, Opposition
9	Individual Keys Exclusive Control
10	Ownership Transfer
11	Account Management & Portability
12	Revocation Lists Management

	Digital softwares list – Sub Contractor Processor
1	Originals of Document Creation Issuance
2	Integrity of Document Certification
3	Timestamp Value Date Certification
4	Traceability Control Certification
5	Signatory Consent of Visible Signature
6	Multilateral Doc & Signatures Exchanges
7	Collaborative Document Encryption
8	Delivery - Correspondence Account Mgt
9	Notary Control& Validation Visible Signature
10	Legal Proof - Probative Value Guarantees
11	Copy Management Processing
12	Accounting or Financial Transfer

IN ONE EXTENDED WORKFLOW and BLOCKCHAIN

DIGITAL CORRESPONDENCE ACCOUNT SECRETY AND MESSAGING

INCLUDING ALLTYPES OF TRANSACTION & DIGITAL SIGNATURE



IDENTIFICATION-RIGHTS
TRUST SERVICES
COMMITMENT CONTACT

DOC ORIGINAL CREATION
UNIQUENESS INFALSIFIABLE
LEGAL DIGITAL SIGNATURES
VISIBLE VERIFIABLE
INTEGRITY TIMESTAMP

DOCUMENT ENCRYPTION

DOCUMENT DECRYPTION

REAL TIME UPDATED : IDENTITY, AUTHENTICATION DEVICE, POWERS, BILATERAL AGREEMENT, PERMISSION.

CONFORMITY ASSESSMENT : DOCUME NT ORIGINAL UNIQUENESS, STRONG CONSENT, REGULATORY SIGNATURES, EVIDENCE VALUE

CONFORMITY: MULTILATERAL ENCRYPTION, CORRESPONDENCE MAILING & TRANSFER
REAL TIME UPDATED : ENTITLEMENT FOR DOCUMENTARY DECRYPTION

TrustSeed SAS Capital € 5.450.000 Office : 49 Bis Avenue Franklin-D-Roosevelt, 75008, PARIS – France
Dc. E. Blot-Lefevre -Chairman – ebl@trustseed.com – 33.607343163.

trustseed

QUALIFIED & APPROPRIATE DIGITAL SOFTWARES (24)

AND

RELATED MANDATORY CONTROL CRITERIA

For 42 Control Criteria on 24 Security Software, there are a total of 500 detailed checks and 2,500 scoring points

			1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
			Identity Management	Authentication Management	Individual Entitlements & Permissions	Documentary Commitment by Signatures	Interchange Agreement & SLA	Data Minimisation/Limitation/Purposes	Data Long-term Conservation	Rights Rectification, Erasure, Opposition	Individual Keys Exclusive Control	Ownership Transfer	Account Management & Portability	Revocation Lists Management	Originals of Document Creation Issuance	Integrity of Document Certification	Timestamp Value Date Certification	Traceability Control Certification	Signatory Consent of Visible Signature	Multilateral Doc & Signatures Exchanges	Collaborative Document Encryption	Delivery - Correspondence Account Mgt	Notary Control& Validation Signature	Legal Proof - Probative Value Guarantees	Copy Management Processing	Accounting or Financial Transfer
17	1.Security Access	C	5	5	5	5	5	5	5	5	5	5	5					5	5	5		5			5	5
24	2.Conformity	O	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
11	3.Pairing Attributes	N	5	5	5		5			5	5	5	5	5					5				5			
18	4.Interoperability	T	5	5	5	5					5	5	5		5	5	5	5	5	5	5	5	5	5		5
9	5.Integrity	R	5	5			5								5	5	5	5					5	5		
8	6.Present value Attributes	O	5	5	5		5			5	5								5				5			
24	7.Traceability	L	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
12	8.Probative value	&	5	5			5								5	5	5	5	5			5	5	5		5
24	9.Real Time	V	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
12	10.Confidentiality	A	5	5	5	5	5	5	5	5	5	5	5	5												
6	11.Keys Self-Control	L									5				5	5		5		5			5			
24	12.Accountability	I	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
1	13.Trustworthy List	D					5																			
5	14.Certification	A	5	5												5	5	5								
24	15.Resilience Recovery	T	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
24	16.Correction	I	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
5	17.Rectification	O	5	5	5		5	5																		
8	18.Notation	N	5	5							5					5	5	5	5				5			
14	19.Erasure						5		5						5	5	5	5	5	5	5	5	5	5	5	5
5	20.Custody		5				5				5								5				5			
24	21.Lawfulness		5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
3	22.Consent					5													5				5			
1	23.Treatment Limitation BC							5																		
12	24.Treatment Finality BC														5	5	5	5	5	5	5	5	5	5	5	5
12	25.Data Minimization BC		5	5	5	5	5	5	5	5	5	5	5	5												
20	26.Prevention		5	5	5		5				5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
3	27.State Safety interest		5	5							5															
6	28.Portability Framework		5	5	5				5		5		5													
1	29.Conservation LCM												5													
2	30.Profiling									5			5													
19	31.Appropriate Guarantees				5	5	5	5	5	5	5	5	5	5	5				5	5	5	5	5	5	5	5
3	32.Opposition					5													5				5			
24	33.Obligation of Result		5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
2	34.Territoriality		5										5													
24	35.Control		5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
1	36.Transparency																	5								
8	37.Exact completeness		5	5	5		5	5			5							5				5				
3	38.Data Updated		5		5		5																			
7	39.Uniqueness		5				5				5				5				5			5	5			
2	40.Data Destruction												5													5
24	41.Alert		5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
24	42.Certification Mechanisms		5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
500	CONTROL CRITERIA																									
2500	CRITERIA QUALITY NOTATION																									
	2.500=		150	130	115	90	135	90	85	90	130	90	115	80	90	100	100	110	135	85	85	100	130	90	80	95

trustseed

PRESENT APPLICATIONS

QUALIFIED & APPROPRIATE DIGITAL SOFTWARES (24)

AND

RELATED MANDATORY CONTROL CRITERIA

For 42 Control Criteria on 24 Security Software, there are a total of 500 detailed checks and 912 scoring points.

Percentage of compliance =36%

			1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
			Identity Management	Authentication Management	Individual Entitlements & Permissions	Documentary Commitment by Signatures	Interchange Agreement & SLA	Data Minimisation/Limitation/Purposes	Data Long-term Conservation	Rights Rectification, Erasure, Opposition	Individual Keys Exclusive Control	Ownership Transfer	Account Management & Portability	Revocation Lists Management	Originals of Document Creation Issuance	Integrity of Document Certification	Timestamp Value Date Certification	Traceability Control Certification	Signatory Consent of Visible Signature	Multilateral Doc & Signatures Exchanges	Collaborative Document Encryption	Delivery - Correspondence Account Mgt	Notary Control& Validation Signature	Legal Proof - Probative Value Guarantees	Copy Management Processing	Accounting or Financial Transfer
23	Security Access	C	5	5	1	4	1	1	2	2	1	0	1													1
38	Conformity	O	5	5	1	2	1	1	1	1	0	0	1	1	1	5	5	0		3		2		1	2	
12	Pairing Attributes	N	2	2	1		1			1	1	0	2	2												
0	Interoperability	T	0	0	0	0																				
18	Integrity	R	3	3			0									5	5	0						2		
14	Present value Attributes	O	5	5	1		0			1	2															
44	Traceability	L	5	5	1	5	1	1	2	2	1	0	3	1	1	5	5	0				2		1	3	
26	Probative value	&	5	5			1								2	5	5	0				1		2		
56	Real Time	V	5	5	1	4	0	2	2	2	2	0	2	2	5	5	5	0		3		5		1	5	
44	Confidentiality	A	5	5	5	5	5	5	5	5			2	2												
10	Keys Self-Control	L									0					5	5									
16	Accountability	I	2	2					2							5	5									
2	Trustworthy List	D					2																			
18	Certification	A	5	3												5	5									
40	Resilience Recovery	T	2	2	2	2	1	0	2	2	1		2	2	2	5	5			2		2		2	4	
50	Correction	I	4	4	3	3	1	2	2	1	1		2	2	2	5	5			3		3		2	5	
16	Rectification	O	5	5	2		2	2																		
18	Notation	N	4	4												5	5									
45	Erasure						5		5						5	5	5			5		5		5	5	
7	Custody		5				1				1															
50	Lawfulness		5	5	3	3	2	1	3	2	1		3	2	2	5	5			2		2		1	3	
4	Consent					4																				
3	Treatment Limitation BC							3																		
21	Treatment Finality BC														3	3	3			3		3		3	3	
35	Data Minimization BC		4	4	3	3	3	3	3	3	3		3	3												
39	Prevention		5	5	3		2						3	2	1	5	5			2		2		2	2	
10	State Safety interest		5	5																						
9	Portability Framework		2	2	2				1		1		1													
3	Conservation LCM												3													
4	Profiling									2			2													
	Appropriate Guarantees																									
5	Opposition					5																				
43	Obligation of Result		2	2	2	2	2	2	2	2	1		3	3	2	5	5			2		2		2	2	
10	Territoriality		5										5													
10	Independent Control															5	5									
14	Transparency		5	5												2	2									
27	Exact completeness		5	5	5		2	1								3	3					3				
12	Data Updated		4	4	2		2																			
24	Uniqueness		5				2				1				3	5	5					3				
5	Data Destruction												5													
45	Alert		5	5	2		2	2	4	2		2	2	2	2	3	3			2		2		1	4	
42	Certification mechanisms		5	5	2	1	2	2	2	1	1	1	2	2	1	5	5			2		1			2	
	MANDATORY CRITERIA OF QUALITY																									
912	**CRITERIA QUALITY NOTATION**																									

912/2500 = 36 %

trustseed

Here are the articles of the two GDPR and e.IDAS regulations that establish the constraints for the 42 Primary Obligations protecting individuals and legal entities in documentary secrecy, the protection of trusted attributes and personal keys, and in the online legal value of original documents and signatures.

	42 FUNCTIONS & QUALITY CRITERIA	GDPR GENERAL DATA PROTECTION REGULATION	e.IDAS ID-DOC SIGNATURE & SEAL
1	Security Access	Art.5.13.15.32	Art.19
2	Conformity COC	Art.40.42.43.58.70	
3	Pairing Attributes	Art.17	
4	Interoperability		Ali.54-Art.7.f
5	Integrity	Art.5	
6	Present value Attributes	Art.40	
7	Traceability	Art.28.30.33.37.57	
8	Probative value	Art.6.40.47	Art. 24.25
9	Real Time	Ali.87.Art.28.2h.66	Ali.61.
10	Confidentiality	Art.5.32.90.	
11	Keys Self-Control	Art.28.39	Art.26
12	Accountability	Art.28.39	
13	Trusted Third Party List	Art.17.	
14	Certification	Art.28.30.42	
15	Resilience Recovery	Art.32.47	
16	Correction Procedures	Art.47	
17	Rectification Rights	Art.7.13. 15.16.19	
18	Notation	Art.25.35.	
19	Erasure	Art13. 15.17.30	
20	Custody		Art.34.
21	Lawfulness	Art.5.6.13.18.82	Art.24
22	Consent	Art.4.7.17.9.13	Art Annexe III.2
23	Treatment Limitation	Art.5.15.18.19.47	
24	Treatment Finality	Art.5.6 .13. 15.28.30.32.35.47	
25	Data Minimization	Art.5.25. 47	
26	Prevention	Art.47	Art.24.1.g.e.Idas.A.II.1d.
27	Safety Public interest	Art.6.23	
28	Portability	Art13.20	
29	Conservation	Art.13.30.	
30	Profiling	Art13. 15.	
31	Appropriate Guarantees	Art13. 28.40	
32	Opposition	Art13.21.	
33	Responsibility Obligation of result	Art.24.28.41	
34	Territoriality	Art3	
35	Independent Control	Art.28.31.33.40.41.e.IDAS.3.40.41-33.1b.	Art. 3.40.41-33.1b.
36	Transparency	Art.5 .7.40	
37	Exact Completeness	Art.5	
38	Data Updated	Art.5	
39	Uniqueness	Art.25.28	Art.3/13/28/.9/1d.III/f. IV/g.Ali.51.Art32.1d.A.III-f.IV.g.
40	Data Destruction	Art.28	
41	Alert	Art.33	
42	Certification Mechanisms	Art.24.25.28.32.40.41.42.70.	

trustseed

Here are the 18 mandatory information that must be summarized in the minutes of signature of each signatory and account holder.

The reference articles for each mandatory mention are mentioned (Lawfulness, Loyalty, Transparency, Traceability).

REGULATORY CONSTRAINTS ON DIGITAL EXCHANGES AND SIGNATURES

	COMMITMENT BY SIGNATURE(S) DIGITAL LEGAL PROOF	RATING	**CURRENT SITUATION PROBATIVE VALUE MEASUREMENT**	GDPR -e.IDAS **PROBATIVE VALUE MEASUREMENT**
1	DIGITAL DOCUMENTARY ACCOUNT NAME -HOLDER	GUARANTEED Art.43-44 e.IDAS	3/5	5/5
2	DIGITAL IDENTITY CERTIFICATE NUMBER & NOTATION	QUALIFIED/GUARANTEED Art.6-7 e.IDAS	4/5 *	4/5 *
3	**TRUST SERVICE PROVIDER MATRICULATION CERTIFICATE FOR WEBSITE AUTHENTICATION**	QUALIFIED Article 45 e.IDAS	5/5	5/5
4	**BILATERAL INTERCHANGE AGREEMENT SENDER/RECEIVER(s)**	GUARANTEED GDPR Ali.32 ; 4/2/11	1/5	5/5
5	**SIGNATORY NAME** AND STATUS (HOLDER or PROXY)	GUARANTEED GDPR Art.5-6	4/5	5/5
6	PDF IMAGE ORIGINAL FILE N° CERTIFIED (INFALSIFIABLE) e.IDAS Art.3/13/28/.9/1d.III/f. IV/g.Ali.51.Art32.1d.A.III-f.IV.g.	GUARANTEED GDPR Art.25.28	2/5	5/5
7	PDF INTEGRITY SEAL INFALSIFIABLE CERTIFIED	QUALIFIED e.IDASArt 35	5/5	5/5
8	PDF TIMESTAMP SEAL INFALSIFIABLE CERTIFIED	QUALIFIED Art.42 e.IDAS	5/5	5/5
9	CONFORMITY VALIDATION CERTIFIED IN PRIVATE BLOCKCHAIN	GUARANTEED GDPR Art.40-41	1/5	5/5
10	PRIVATE DIGITAL SIGNATURE OF CONSENT VISIBLE VERIFIABLE Art.28.30.33.37.57.40.41 GDPR	GUARANTEED Art.25.26.32.33. e .IDAS Art.7.9.13. GDPR	0/10	10/10
11	SIGNATORY PUBLIC VERIFICATION KEY	GUARANTEED Art.28.3930.33.37.57 GDPR	0	5/5
12	PRIVATE DIGITAL SIGNATURE MATRICULATION	GUARANTEED Art.28.3930.33.37.57 GDPR	0	5/5
13	SECRET DOCUMENTARY BY ENCRYPTION & PROTECTED KEYS	GUARANTEED Art.5.32.90.GDOR	0	5/5
14	DOC EXCHANGE/TRANSFER WITH XML RESEARCH INFO ENGINE.	GUARANTEED Art24-28-31-44-46.47 GDPR	0	5/5
15	PERSONAL NOTARY SIGNATURE OF EVIDENCE VALUE	GUARANTEED Art.40.41 GDPR Art.13.33 e.IDAS	0	5/5
16	NOTARY PUBLIC VERIFICATION KEY	GUARANTEED Art.28.3930.33.37.57 GDPR	0	5/5
17	NOTARY DIGITAL SIGNATURE MATRICULATION	GUARANTEED Art.28.3930.33.37.57 GDPR	0	5/5
18	MULTILATERAL PRIVATE BLOCKCHAIN VALIDATION NUMBER	GUARANTEED Art.24.28.40-41-44-47 GDPR	0	5/5
	NOTATION FROM QUALIFIED VALIDATION PARTY n° Liability and burden of proof Art.13		30/100 30 %	99/100 99 %

***-Complementary verification of accuracy by a "doubt clearance procedure" using official servers and databases.**

trustseed

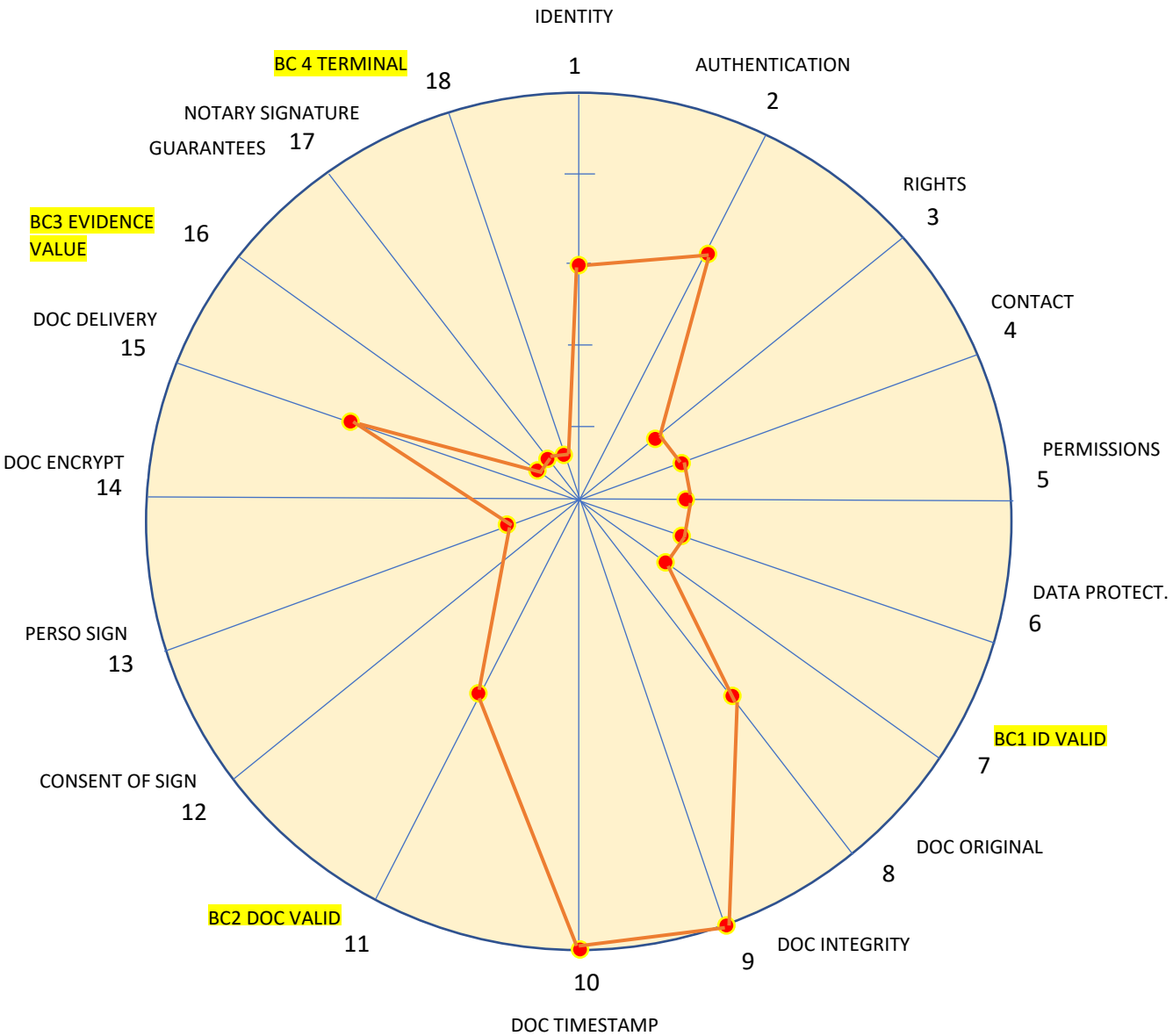
LEGAL CONFIRMATION OF DIGITAL EXCHANGE AND SIGNATURES

	COMMITMENT BY SIGNATURE(S) DIGITAL LEGAL PROOF	SENDER 1 SIGNATORY S1 SIGNATORY S2	**RECEIVER 2** SIGNATORY S1 SIGNATORY S2	**RECEIVER 3** SIGNATORY S1 SIGNATORY S2
1	DIGITAL DOCUMENTARY ACCOUNT NAME -HOLDER	X	X	X
2	HOLDER DIGITAL IDENTITY CERTIFICATE NUMBER & NOTATION	5	4	4
3	NATIONS	FRANCE	CHINA	SAN DOMINGO
4	RESPONSIBLE OF TREATMENT : TRUST SERVICE PROVIDER MATRICULATION CERTIFICATE FOR WEBSITE AUTHENTICATION	X	X	X
5	COUNTERPARTIES BILATERAL INTERCHANGE AGREEMENT	X	X	X
6	SIGNATORY NAME AND STATUS (HOLDER or PROXY)	P	H	P
7	PDF IMAGE ORIGINAL FILE N° CERTIFIED (INFALSIFIABLE)	X	X	X
8	PDF INTEGRITY ELECTRONIC SEAL INFALSIFIABLE CERTIFIED	X	X	X
9	PDF TIMESTAMP ELECTRONIC SEAL INFALSIFIABLE CERTIFIED	X	X	X
10	TRACEABILITY - CONFORMITY CONTROLS VALIDATION /PRIVATE BLOCKCHAIN	X	X	X
11	CONSENT OF SIGNATURE VISIBLE VERIFIABLE QS = QUALIFIED SIGNATURE AS = ADVANCED SIGNATURE	S1/QS S2/AS	S1/QS S2/AS	S1/AS S2/QS
12	SIGNATURE PUBLIC KEY VERIFICATION	X	X	X
13	DIGITAL SIGNATURE STATUS : Q= QUALIFIED A= ADVANCED	Q	A	A
14	Certification Authorities or Control : Qualified Signatures	CA n°1	CA n°2	CA n°3
15	Control and Validation Body CVB Art.40-41 (GDPR) : Advanced Signatures	CVB 1	CVB1	CVB1
16	PROTECTION DOCUMENT/ENCRYPTION – and KEYS/ACCOUNT/SIGNATORY	X	X	X
17	DOC EXCHANGE or FINANCIAL TRANSFER WITH XML RESEARCH INFO ENGINE.	X	X	X
18	NOTARY SIGNATURE : EVIDENCE VALUE CERTIFICATE SIGNED	X	X	X
19	NOTARY PUBLIC KEY VERIFICATION	X	X	X
20	NOTARY DIGITAL SIGNATURE QUALIFICATION	CA n°1	CA n°1	CA N°1
21	MULTILATERAL PRIVATE BLOCKCHAIN CONSOLIDATION	X	X	X
22	EVIDENCE VALUE NOTATION FROM QUALIFIED VALIDATION PARTY (n°) Liability and burden of proof Art.13 e.IDAS	X	X	X

9 out of 10 people do not have a qualified identity, ie 100% reliable. This is not a reason to prevent these people from signing. The need of the market is to allow everyone to sign their exchanges without being prevented from doing so if their counterparties have a qualified identity distinct from theirs in terms of rating and operation. There are many ways to verify the probative value of stakeholders in signing a commitment to establish traceability and sufficient evidence. Enabling everyone to sign with variable and measurable identities encourages people to protect themselves to adopt a so-called skilled identity. The interoperability of identities and means of authentication, consent and signature contributes to the development and security of national and global commercial and financial exchanges.

Characteristics	SENDER Signatory 1	SENDER Signatory 2	Receiver 1 Signatory 1.1	Receiver 1 Signatory 1.2	Receiver 2 Signatory 2.1	Receiver 2 Signatory 2.2
Identity Rating	3	5	5	5	4	5
Advanced Signature	Control Body Art.40-41 GDPR				Control Body Art.40-41 GDPR	
Qualified Signature		Certification Authority Country 1	Certification Authority Country 2	Certification Authority Country 2		Certification Authority Country 3
Signature Object Condensate Signed	Visible	X	X	X	Visible	X
Public Key	Visible	X	X	X	Visible	X
Complementary Information	Visible	X	X	X	Visible	X
Verification	X	X	X	X	X	X

Current level of legal and computer security of documents and signatures online



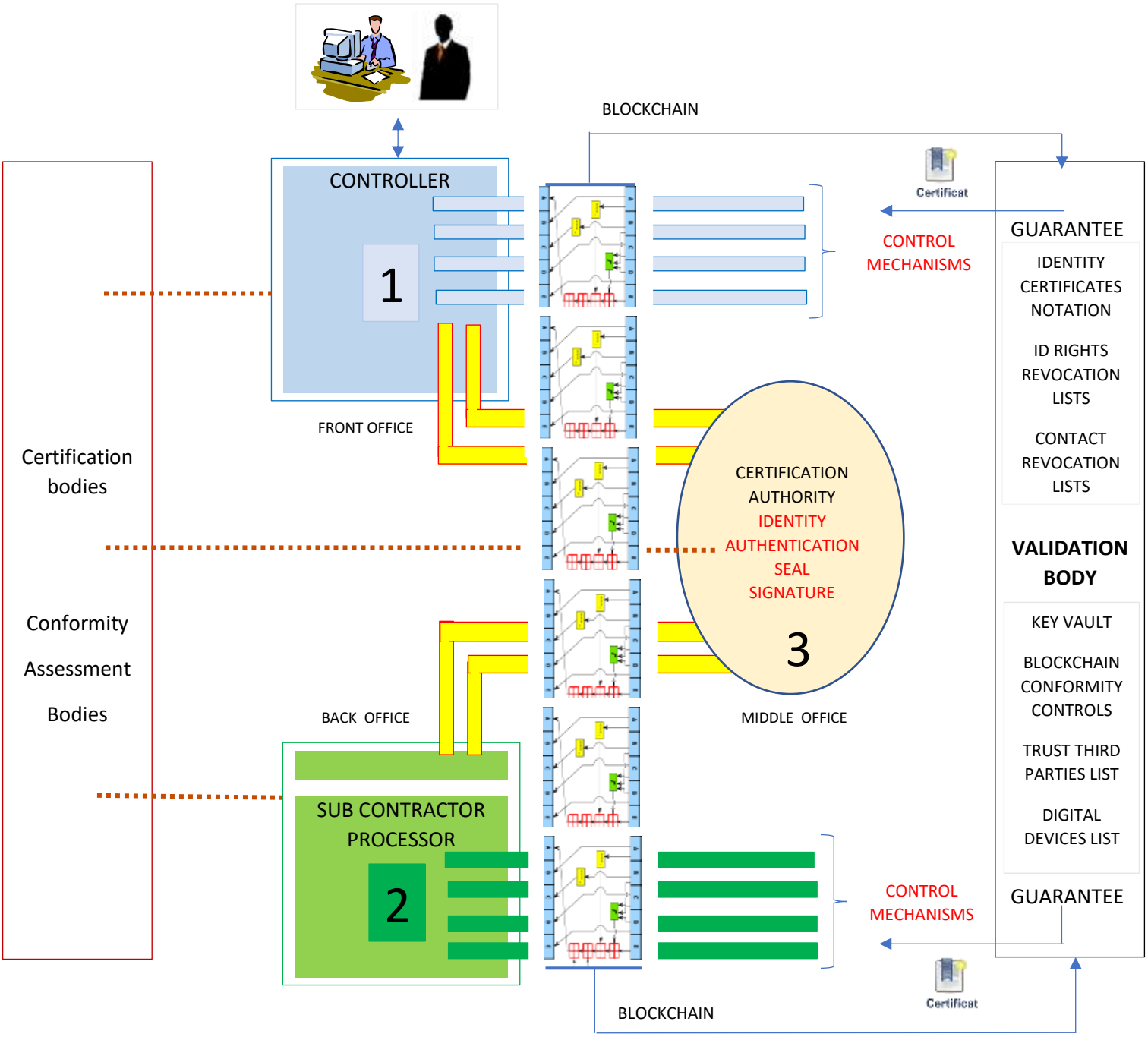
The area of croissants is calculated according to the level of risk in legal and computer security

BC = Blockchain n°1-2-3-4

trustseed

Trinary Architecture of Security and Digital Trust

Combination of the services of Certification Authorities with the technical and organizational means of a Controller with one Subcontractor Processor



CERTIFIED SOFTWARES USING APPROPRIATE TECHNICAL & ORGANIZATIONAL MEANS WITH CONTROL MECHANISMS SUBMITTED TO VALIDATION BODY TO OBTAIN PROBATIVE VALUE GUARANTEES

QUALIFIED DEVICES INCLUDING SECURITY GUARANTEES

TrustSeed SAS Capital € 5.450.000 Office : 49 Bis Avenue Franklin-D-Roosevelt, 75008, PARIS – France
Dc. E. Blot-Lefevre -Chairman – ebl@trustseed.com – 33.607343163.

The security and digital trust workflow can be described simply. This security includes a set of electronic stamps to guarantee the integrity of certificates, timestamping and traceability, as well as personal consent signatures: signatures of the signatories, signature of the sworn employee to sign the certificate of probative value signed and encrypted exchanges.

	Trusted PARTIES	TRUST SERVICE MANDATE			PROCESSOR SUB CONTRACTOR				SIGNATORY	CONTROL VALIDATION BODY		
	STEPS	IDENTITY REGISTRY	IDENTITY QUALIFIED	AUTHENTICATION @	ORIGINAL DOCUMENT CREATION	INTEGRITY DOCUMENT SEALED	TIME STAMP SEALED	BLOCK CHAIN SEALED I	PERSONAL CONSENT SIGNATURE	BLOCK CHAIN SEALED II	NOTARY VALIDATION SIGNATURE	BLOCK CHAIN SEALED III
1	INDIVIDUAL Or EMPLOYEE											
2	FILE DOCUMENT											
3	VALIDATION 1											
4	SIGNATORY											
5	FILE ENCRYPTION											
6	VALIDATION 2											
7	NOTARY											
8	BLOCKCHAIN TERMINAL											

Enumeration of the stamp, signature and encryption keys used in a document exchange

	TYPES OF KEYS	HOLDER PROXY	CONTROLLER RESPONSIBLE OF TREATMENT	SUB-CONTRACTOR OPERATOR PROCESSOR	CONTROL & VALIDATION BODY INDEPENDENT CONTROL MECHANISMS APPROPRITE GUARANTEES	CERTIFICATION AUTHORITIES ID CERTIFICATE ID AUTHENTICATION PORTAL SEAL SIGNATURE
1	PORTAL @ SEAL		Qualified Cert.			KEY Root Certification
2	ID CERTIFICATE SEAL	Qualified Guaranty			REGISTRY KEY SERVER	KEY Root Certification
3	SEAL OF VALIDATION		GUARANTY		VALIDATION KEY SERVER	
4	ORIGINAL UNIQUENESS SEAL	GUARANTY		KEY		KEY Root Certification
5	ORIGINAL INTEGRITY SEAL	GUARANTY		KEY		KEY Root Certification
6	ORIGINAL TIMESTAMP SEAL	GUARANTY		KEY		KEY Root Certification
7	SEAL OF VALIDATION			GUARANTY	VALIDATION KEY SERVER	
8	PERSONAL ID CONSENT SIGNATURE	Advanced Sign. Certi.	Advanced Sign. FACILITIES	Advanced Sign APPLICATION	ADVANCED PERSONAL KEY SIGNATURE CUSTODY	
9	DOC CONFIDENTIALITY ENCRYPTED	Advanced KEY. Certi.	Advanced KEY FACILITIES	Advanced KEY ENCRYPTION	ADVANCED KEY ENCRYPTION CUSTODY	
10	SEAL OF VALIDATION			GUARANTY	VALIDATION KEY SERVER	
11	EMPLOYEE NOTARY SIGNATURE	Advanced Sign. Certi.	Advanced Sign. Validation	Advanced Sign APPLICATION	ADVANCED NOTARY KEY SIGNATURE CUSTODY	
12	TERMINAL BLOCKCHAIN				VALIDATION KEY SERVER	

General conclusion

The legal and informational security of digital exchanges brings to the "management files" established by the business software, the mandatory levels of certification or guarantees that are appropriate and indispensable to certify in real time between the signatories of the exchange, the authenticity of their identities and their powers, and to establish the uniqueness and integrity of the documents and personal signatures created at their request.

This legal and informational security of digital exchanges also provides "management files" with the appropriate technical and organizational means for the exercise of all individual and regulatory rights concerning confidentiality, pseudonymisation, rectification, deletion and portability.

In this way the "management files" are transformed into “binding official documents”, into "commitment by signature" of accounting, fiscal, legal or financial nature; they are effectively enforceable against third parties, and their digital evidence can be legally enforced before the Courts.

For the protection and transfer of personal data, for the exclusive control of personal signature keys by consent and documentary secret by encryption, and for the faithful transformation of "management files" into "tamper-proof and certified digital files including probative value" all the necessary preventive measures, guarantees and technical means are taken by the Controller.

The Controller is a front office, a Trust Service Body who must permanently preserve the identity of the people, check the current validity of their rights and personal contacts, as well as maintain the conservation of the signed exchanges and the confidentiality of the encrypted data.

Pursuant to Articles 24, 28 and 29 of the GDPR Regulation, the person (Controller) responsible for the processing of a "management file" used for a digital exchange (commercial or financial commitment by signature) is the only one able to determine the purposes and means of processing the "management file" to dematerialize its bilateral, multilateral or cross-border document exchange, between the signatory parties or with the recipient parties.

These aims and technical means are implemented by a chosen and qualified subcontractor. This subcontractor implements all the technical and organizational means whose results are verified, certified, or guaranteed from the control mechanisms used by an independent validation body, responsible for the digital application of the code of professional conduct (Art. .40 GDPR).

Under Article 29 GDPR, processing by the Subcontractor who has access to personal data (Management File), may only be processed under the authority of the Controller.

Finally, Article 89 of the GDPR Regulation stipulates that any Controller who has participated in the processing is liable for the damage caused by the processing which constitutes a violation of this Regulation (Art.29 GDPR).

A subcontractor shall be held liable for the damage caused by the processing only if he has not complied with the obligations laid down in this Regulation, obligations which are specifically incumbent on the subcontractors, or in the case he has acted outside the lawful instructions of the Data Controller or contrary to them.

trustseed

At the end of the day, we can very easily summarize the 10 legal and IT security constraints that apply, in commercial and financial exchanges, on the one hand to the online management of identities, and on the other hand to the management signed documentary exchanges:

For identities, the 10 principles to be respected jointly are:

1. National Identity Certificate uniqueness under the control of a Nation,

   Single Subsidiary Certificates uniqueness under the control of qualified Communities

2. Attributes-credentials -protected personal Codes (hash)

3. Signature and encryption keys under exclusive control and by consent

4. Powers, Real-time updated Powers of Attorney

5. Permission - Professional Qualification - updated by each Community

6.Contact: consent and update conditions

7. Data: protection, minimization, limitation

8.Services: Commitments by signature (s) and transfers

9.Rights: rectification, deletion, pseudonymisation, opposition

10. Portability, interoperability, resilience

Regarding the digital transformation of management files, there are also 10 rules:

1. Original documentary: guarantee of uniqueness, instant verification

2. Document file: guarantee of integrity, instant verification

3. Date of value: timestamp uniqueness and integrity

4. Consent: manifestation, traceability - causality

5. Signature: uniqueness, integrity, visible, verifiable always

6. Controlled and validated multilateral conformity assessment

7. Collaborative Document Encryption

7. Proof of correspondence: e-mail account

8. Proof of Transfer of Ownership: Securities Account

9. Individual signature of validation and probative value: appropriate guarantees

10. Traceability - Consolidated validation in private blockchain

Trade security is a real challenge as the conception of title deeds (Identity, transaction, contract, security, financial instrument, currency, etc.) is realized "ipso facto" in SaaS, in PaaS, in Cloud Computing , without any more recourse (back) to the management and the physical control (Visual controls and manuals).

The current dematerialization is not criticizable, even if it is still unreliable. Indeed, the considerable acceleration of national and international exchanges has led to mass processing whose security and performance can only be controlled by the security of trade as organized, for example, by the GDPR regulation with the regulation e.IDAS regarding "Online" signature.

These two regulations are essential to the security of digital exchanges. And the lack of knowledge about how strong authentication, sealing, signing and encryption works, explains some of the current holes in security.

Another shortcoming comes from the means of real-time control of identities, powers, contact and signature consents, and private key protections.

These technical and organizational means must be accompanied by synchronized control mechanisms verified in blockchain by an independent control and validation body, responsible for the application of professional codes of conduct (Commerce, Banking, Health, Transport, Leisure, Food, Agriculture, Administrations, Customs, ...).

Digital transformation is also the best way to empower natural and legal persons in eco-systems run by Communities with digital codes of conduct.

This digital transformation will also profoundly change the way of leading or driving the entire economy.

Digital transformation is also the new passport to protect trade, especially when the parties are mobile or far apart.

Paradoxically, users can be better served and protected by qualified economic agents and far than by local providers, lacking knowledge or digital experience.

In the near future, the selection of competent market players in digital exchanges will be based on certification criteria for security software, and on the legal qualification of trusted services, responsible for processing, and capable of applying digital codes of conduct .

This draconian selection at the global level is the price to pay to protect Consumers and States increasingly exposed to uncontrolled risks. This is the price to pay to reduce the economic risks that the States always learn at their expense the cost of the bill and the social fracture.

These digital exchanges, which are progressing considerably, will be controlled by a few key players (fewer than perhaps the number of Countries in the world), and more than 30% of the volume of these exchanges will be cross-border and controlled at long distance.

In these conditions, we understand the challenge of e-commerce and digital finance whose means of regulation and resilience must necessarily develop prevention in all ecosystems and between Communities and responsible Nations. In this evolution that gives a premium to qualified Operators, able to overcome technological barriers, a new passport for commercial and financial intermediation is emerging which will no longer be given to everyone, and without severe financial conditions.
