eBook_ Caratteristiche di sicurezza e interoperabilità delle firme grafometriche

Gruppo di Lavoro AIFAG 2014-01

Caratteristiche di sicurezza e interoperabilità delle firme grafometriche

Coordinatori*: Franco Ruggieri (Consiglio Direttivo e Comitato Scientifico AIFAG) e Giovanni Manca (Comitato Scientifico AIFAG)*

Hanno contribuito alla redazione del documento finale:

Simone Baldini (Aruba Pec S.p.A.)

Andrea Caccia (Libero professionista)

Valerio Cristofaro (Postel S.p.A.)

Marco Cuniberti (Studio Legale Costa Cuniberti)

Alfredo Esposito (Infocert S.p.A.)

Stefano Flaim (HiT – Internet Technologies S.p.A.)

Antonella Foi (Grafologa Forense – Dir. Naz. AGI – Comitato Scientifico AIFAG)

Stefano Maestri (Sygest Srl)

Monia Marziale (Unimatica S.p.A.)

Mauro Mattioli (Unimatica S.p.A.)

Eugenio Stucchi (Direttore del Comitato Scientifico AIFAG e notaio)

Luigi Tomasini (Namirial S.p.A.)

Andrea Valle (Comitato Scientifico AIFAG)

A.I.F.A.G. ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA

eBook_ Caratteristiche di sicurezza e interoperabilità delle firme grafometriche

AIFAG Work Group 2014-01 on *"Security and interoperability of Handwritten Biometric Signatures"*

N.B. Il presente documento è stato redatto in lingua inglese al fine di poterlo proporre agli organismi europei di standardizzazione, nonché di consentire loro di produrre specifiche e standard.

AIFAG Associazione Italiana Firma Elettronica Avanzata Biometrica e Grafometrica
Sede Legale: via Mario Stampacchia 21 - 73100 Lecce - C.F: 93124220752 - E-mail: info@aifag.it

15 June 2015

Contents

1) Forewords

The Italian AIFAG (Associazione Italiana Firma elettronica Avanzata, Grafometrica e biometrica – Italian Association for electronic Advanced and handwritten biometric signature) started on 2014-12-05 a Working Group with the purpose of drafting one standardisation proposal to be forwarded, eventually, to EU standardisation bodies. The present document is the result of that effort, finalised on 06/15/2015.

2) Introduction

Starting from 2007 in Austria, from 2009 in Spain, from 2011 in Italy, a new strain of Advanced Electronic Signature began to spread quickly. This new AdES type, is called with different names, so it can be assigned the name of "Handwritten Biometric Signature" – HS. One handwritten biometric signature is created by applying the signatory's handwritten signature by means of specific biometric devices (tablets, biometric pens, etc.). These devices capture both the signature image and the related biometric measures[1], called "channels" in Standard ISO/IEC 19794-7. These channels are securely transmitted from the signing device to a processing unit where an application elaborates signature image, channels and document to be signed, basically through hashing and encryption, according to specific and usually proprietary procedures.

The outcome of the process is applied or logically attached to the document to be signed, thus producing a HSed document. This document, in addition to being distributed to the interested persons, should also be securely transmitted to a secure preservation system under the responsibility of the organisation providing its users with the HS system.

In case the signature is questioned, a verification procedure is implemented, generally based on the following basic steps: the encrypted data, in particular the signature channels, are decrypted and the purported signer applies a certain number of

[1] By "biometric measures" it is intended in this context all biometric data related to the affixed handwritten biometric signature usable for generating or verifying a handwritten biometric signature.

handwritten biometric signatures using a suitable device. From these handwritten biometric signatures a channels template is derived and a graphologist assesses the compatibility with this template of the just decrypted channels, thus assessing the HS authenticity. The document integrity is verified too, since the hashed and encrypted information, generated by the HS creation procedure, are such that it can be detected if the document has been modified. Alternatively, decrypted channels can be compared with a number of handwritten biometric signatures issued by the signatory at time of signing with a suitable device. It is recommended, in case of particularly important documents or of long terms relationships, for example in case of a bank, that the signatory issues a number of handwritten biometric signatures suitable to create a template.

This HS has the advantage to allow people, not equipped with tools capable to generate Qualified Electronic Signatures, to create an Advanced Electronic Signature conformant not only with the EU Directive 1999/93/EC, but also with the recently issued EU Regulation 910/2014; this AdES therefore has legal common ground in all EUMS. Unfortunately nowadays specific national rules apply in some Member States that do not allow cross border recognition of HSs. European standards can be the basis for cross border recognition and some degree of interoperability for HSs, if referenced by specific EC implementing acts according to article 27(5) of the Regulation (EU) n. 910/2014[2]. One thing that is to be highlighted is that in some EUMS legislations (e.g. in Italy) AdES is legally valid only within the domain of the entity that made the AdES solution available to its users. This is easily understandable in the HS case, where the decryption private key and the HS creation process are, on principle, peculiar to one AdES solution. It is to be noted that the domain at issue could be a multinational environment, as in the case of banks, insurance companies, etc.

As in any Electronic Signature, though, specific security measures are necessary, in order to prevent malicious capture of the signature image and of the channels, and the creation with them of fake HS affixed to documents in order to arbitrarily attribute them to a presumed signer that is, instead, totally unaware of them. As typical in security matters, there is always a risk that the malicious capture is possible. This risk must be evaluated considering the operating scenario and the awareness of the user towards the tools that is using.

[2] In Italy DPCM 22/2/2013 addresses AdES in articles from 55 through 61

However is fundamental to keep in mind that 100% security does not exist.

Another issue is interoperability. As of now, no common or standardised HS creation and verification procedure exists, so each HS solution implements, on principle, its own proprietary HS creation procedure. Consequently, one entity that provides its customers or users with one specific HS solution will have serious difficulties to move to a different solution, since the HS verification procedure of this second solution might not, again on principle, be suitable to verify a HS created with the previous one.

Another issue to be taken into account concerning "interoperability" is related to decryption. The HS creation process usually encrypts with an asymmetric algorithm a number of data, including channels. HS verification, that implies decryption, therefore requires usage of a specific decryption key. Since each solution might have one specific decryption key, when moving from one HS solution to another the new decryption key might be different. Therefore any HS created with a specific solution would require the decryption key of that very solution. This hindrance could be overcome, though, by summoning the physical or legal person to whom the "first" decryption key is entrusted whenever necessary. Obviously, if the second solution adopts the same encryption key as the previous one, this problem wouldn't exist, but this depends on the specific HS service contracts.

In conclusion: there is a strong need to standardize the entire handwritten biometric signature process, including the related security measures, so that:

1) Users can have sufficient trust on the efficaciousness of the HS solutions they adopt;
2) Users can have sufficient trust on the security, and therefore on the reliability, of the HS solutions they accept;
3) Organisations providing their users with HS solutions developed by external companies, can with limited difficulties move from one HS solution to another, thus improving the overall marketplace interoperability.

The purpose of this paper is therefore to highlight the issues to be addressed by such standardization effort, leaving the actual standardization activity to official standardization bodies. Moreover, it is a firm belief of the WG that drafted the present paper that such bodies should be the European ETSI and CEN, respectively for the procedure and the security related issues, in order to give way to HS procedures enforceable throughout the whole EU.

Note: The AIFAG WG 2014-01remarked that in some cases there has been some confusion between "handwritten biometric signature" and "Authentication through handwritten biometric signature". This confusion depends on both mechanisms making use of roughly the same biometric signature measures collected via similar devices. It has therefore been deemed as useful, if not utterly necessary, to clarify the differences between HS and "handwritten biometric signature based authentication" (graphoPIN).

As far as the HS procedure is concerned, a first hint has been previously given and it will be dealt in depth in the present document.

As far as Authentication through handwritten biometric signature is concerned, instead, a brief description is given henceforth, with the purpose to highlight its main differences with HS.

In order to subsequently authenticate at one system, the involved person is first enrolled to the same system by applying a number of handwritten biometric signatures on a biometric device from which a template is created to be preserved at the same system. When the same person later on wants to authenticate herself at the system at issue, this person applies her signature with a device similar to that used at enrolling phase, which extracts the channels; a procedure then checks these channels against the template built at enrolment time.

It is now apparent the difference in procedure and in purpose between a HS and an authentication system based on handwritten biometric signatures: the HS application does not necessarily require a previous enrolment, with the exception of what is explained at Clause 6.5) Encryption keys and channels protections, while an authentication mechanism based on handwritten biometric signatures implies no ex post verification.

A final comment on this issue, in addition to what is explained at Clause 6.5) Encryption keys and channels protection: in some sensitive environments, (in a bank, for example), it would be sensible to couple both HS and authentication based on handwritten biometric signature. This way, the bank would previously enrol its customers, and afterwards, in one "shot", it would identify them via their handwritten biometric signature prior to accept their signature as a valid HS to be affixed to a document.

It is also evident that maintaining an archive of HS biometric data and templates and transferring HS channels or using them within what can be called a "Signature Verification Automatic System" introduces several vulnerable points and requires an additional effort to cope with the related security risks.

3) Reference

(1) EU Regulation 910/2014 - REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

(2) ISO/IEC 19794-7 – Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data

4) Definitions and Abbreviations

4.1) Definitions

Advanced Electronic Signature: an electronic signature which meets the requirements set out in Article 26 of EU Regulation 910/2014. (EU Regulation 910/2014)

Channel: data item (captured, intermediate, or processed) recorded in form of a time series

EXAMPLE pen tip position x and y coordinates, pen tip force, pen tilt along the x and y axes, pen azimuth, pen elevation, pen rotation

(ISO 19794-7)

Qualified Electronic Signature: advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures (EU Regulation 910/2014, art. 3, paragraph 11)

Suitable device: a device capable to capture the same channels as the one originally used to apply the original handwritten biometric signature, in a compatible manner.

4.2 Abbreviations

AdES Advanced Electronic Signature

EUMS European Union Member States

HS	Handwritten biometric Signature
HSed	Handwritten biometrically Signed
QES	Qualified Electronic Signature

5) Security levels

Consistently with what is specified in Regulation (EU) 910/2014, Art. 8 Assurance levels of electronic identification schemes, it is recommended to envisage two security levels: High e Substantial.

Note: One example of High Security level measure would be acquiring a number of HSs through a suitable device, at least prior to affixing the handwritten biometric signature from which a HS would be created. Either from these signatures a template could be created or these signatures could be kept as such.

This way it would not be necessary to summon the purported signatory if a HS verification procedure is to be processed. This would turn out very useful in case the signatory, for any reasons, could not actively participate to the verification procedure.

Instead: Substantial security level measure would not require such preliminary process. For example in case of cash depositing at a bank counter.

6) Handwritten biometric signature

6.1) General issues

This clause further elaborates, yet summarily, on the principles briefly described in the Introduction.

Going more in depth on what has been previously sketched, further comments will be made in this clause on the following items:

1) Biometric information collecting devices
2) Transmission link from device to HS creation procedure:
3) HS creation procedures and systems
4) HSed documents preservation.

A more in depth analysis, yet not exhaustive, on what is being presented in items 2) and 3) is available at clauses 9.8.1 HS creation and 9.8.2 HS verification. Other topics, among which encryption/decryption key management and HS verification, are dealt with in other clauses of this document.

6.2) Biometric information collecting devices

A number of devices exist, called shortly "bio-devices", that can be grouped in the following major groups of channels capturing devices:

a) Specific devices that present to the signer the whole document to be signed plus a field where he/she can affix, with a specific "pen", a HS;
b) Specific devices that submit to the signer only the field where the HS is to be affixed with a specific "pen", relying on other means, e.g. a computer screen, for presenting to the signer the document to be signed;
c) General purpose devices, like those usually called "tablets", equipped with screen and SW suitable to capture HSs channels, as well as to present the subscriber the document to be signed;
d) Specific devices similar to a ball tip pen, that can actually apply or not a wet signature to a paper document; these devices can capture the channels in both usage modes (wet or dry signature).

All these devices collect some or all of the data that are defined in standard ISO/IEC 19794-7 as "channels", and forward them to the computer application that actually creates a HS. This forwarding should be secured and, similarly, the biometric devices should securely erase these data as soon as they are no more necessary to the HS creation.

6.3) HS creation procedures and systems

Once the biometric device has gathered the channels and the signature image, it sends them via a secured link to an application within a computer. In the case of tablets, as per clause 6.2) Biometric information collecting devices item c), this connection is entirely internal to the tablet, so this case is to be addressed separately as concerns the transmission security.

This application processes the received data, plus the document to be signed, that the hosting computer would have already acquired, using digest algorithms and common practice encryption techniques based on asymmetric algorithms, according to a sequence that may differ for each HS solution. The involved computer should be protected from intrusions, like malware of any kind, and from tampering.

6.4) HSed documents preservation

Once a HS is affixed or logically attached to the related document, this signed digital object will be dealt with as required by the specific procedure. For example: one copy will likely be delivered or made available to the signer, another should be securely and reliably kept by the organization within which the subscriber has signed with the specific HS solution.

It is of paramount importance that documents signed with a HS are securely and reliably kept in a preservation system because this would ensure:

a) that these document, that do matter for the organization providing the HS solution, are not lost or damaged, so they can easily be retrieved unchanged whenever necessary;
b) that only regularly signed documents are kept. In other words: should an attacker succeed in fraudulently capturing HS channels and in building a fake HSed document, being this document not stored in the organisation's archive it would easily be identified as a fake, since it would not be possible to find a copy of it in the archive.

Therefore the link between the HS creation application and the secure storage / archive should be secured, to prevent damages, alterations, abusive insertions to the archive.

6.5) Encryption keys and channels protections

In some cases it can be necessary to verify HSed documents after a very long time, even after several decades, which might affect the used encryption keys strength. To this regard, the used encryption key length should be assessed taking into account the ETSI TS 119 312 recommendations.

It's possible that the HSs documents are to be verified after a time period longer than what is envisaged in ETSI TS 119 312. In such cases it can be useful to provide for security measures, to limit the risk of brute force attacks to the used encryption.

6.6) Informing signers of the decryption key holder’s identity

The identity of the natural or legal person to whom the decryption private key is entrusted should be formally communicated to involved subscribers. Such information is, indeed, key to let subscribers assess this key issue of the HS solution’s reliability.

Therefore, the HS creation applications should obtain in a secure way the public key to be used to encrypt sensitive information making up a HS, as well as the decryption private key holder’s identity. Such identity should be reliably presented to subscribers when affixing the HSs from which channels are extracted to create this signature.

One possible solution to the above is to have Qualified Trust Service Providers issue Qualified Encryption Certificates related to such public keys. Such certificates would, in fact, provide users with sufficient guaranty on the decryption private key holder’s identity.

7) Encryption/decryption key management

A HS creation process implies a certain number of cryptographic operations, including hashing and asymmetric encryption. The purpose of the latter, i.e. asymmetric encryption, is twofold: ensuring on the one hand the channels confidentiality (indispensable to prevent abuses) and, on the other hand, that the procedure is wisely built, ensuring, as per Regulation EU 910/2014 art. 26, letter (d), that the HS “*is linked to the data signed therewith in such a way that any subsequent change in the data is detectable*”.

This encryption is asymmetric, since it enables a much easier protection of the encryption / decryption key than a symmetric encryption. The private key of the encryption key pair is securely kept by one trusted third party.

There are the following issues on this topic:

1) It is to be ensured that the public key, used by the encryption procedure during the HS creation to protect the data, actually corresponds to the private one held by the trusted third party;
   Note: the Italian Data Protection Authority issued a Regulation on 12/11/2014 requiring that the HS public encryption key is to be kept in a certificate issued by a qualified trust service provider issuing qualified certificates, in

order to provide users with the assurance that the public key actually matches the private key securely kept by the trusted third party.

2) It is to be ensured that the private key cannot be tampered with by any person, not even by the trusted party holding it;
3) It is to be ensured that, should the private key become unusable (damaged or lost), a backup solution exists to decrypt the previously encrypted data;
4) It is to be ensured that the private key can only be activated in a secure way, e.g. with the cooperation of at least two persons without any formal or factual link between them.

Note: As far as previous item 3) is concerned two possibilities exist:

i) The private key is securely backed up and all copies are securely stored in a non tamperable way;
ii) Encryption is made with more than just one key pair, so that what was encrypted can be decrypted with any of the corresponding private keys.

Item i) drawback is that to each backup copy security measures are to be applied to prevent misuse, but the advantage is that, if suitably handled, from each copy additional ones can be produced, making de facto impossible not to be able to decrypt.

Item ii) drawback is that should, theoretically, all these different private keys become unusable, no decryption would be possible. It is a very unlikely event, though, if these private keys are securely kept by different persons in different places.

The public key should be securely inserted into the HS creation application, in order to prevent fake public keys from being used by the same application. There should be, therefore, a mechanism to allow the said application to ascertain that the public key is the correct one. This can be implemented in several ways. Just to make two examples:

a) The public key could be managed by a "trusted officer" and inserted in the HS creation application working area where will be used in a trusted way;
b) The certificate containing the public key could be inserted by a trusted officer into a secured area, securely accessed by the HS creation application.
In this case it would be also possible for the same trusted officer, as an additional security measure, to insert into the HS creation application the certificate

identifier, so that the HS creation application can verify that the certificate in the secured area matches the identifier.

The private decryption key should only be used and activated to decrypt the channels, among other things, when there is a questioned HS to verify. The decryption private key handling is further dealt with in clause 11).

8) Channels

Standard ISO/IEC 19794-7 specifies what channels relate to a HS.

It is advisable, though, that just a limited set of channels are required as mandatory to create a HS. This would allow an easier migration from one HS solution to another. Each solution would be able, though, to take into account additional channels at its will, but, if the "core" channels set is within the set of adopted channels, any other HS solution would be able to verify a signature created with the first HS solution, based on the core channels set. It should be possible for any verification application to identify and extract each and all the channel data included in the HS.

9) Interoperability with ISO Standard

9.1) Foreword

The purpose of this chapter is to analyse and describe one methodology suitable to make interoperable the biometric data representations acquired with the different HS solutions currently present in the market. The proposed solution is based on already available standards.

9.2) Context

At the time the present document is released each of all software houses active in the Italian market have implemented their biometric data representation in an autonomous way, due to lack of standards and of agreements among solution producers, suitable to allow for interoperability, at least up to a certain level.

This situation, in case of litigation, has as a strong limitation that each HS solution is to be interpreted by the graphologist expert using tools provided for solely by the software house that developed the signature solution.

Among the consequences of this situation are:

- The graphologist's objective dependence, in order to perform his expertise, on tools forcibly provided by one specific producer;
- Scant possibility for the graphologist to be aware of and to experiment the different analysis tools available, which has as a consequence a high risk of producing an expertise of limited quality;
- Objective impossibility to assess the different analysis tools quality, given the impossibility to formally apply them on the same data set and to compare the outcomes;
- Substantial risk of impossibility to perform an expertise if, years after a signature creation, the originally provided specific tool turns out to be ineffective.

In such context the intended objective of this document is to define a common set of signature biometric data representation rules suitable to allow reading them when picked up in one common format by different providers tools.

9.3) Biometric Data Encryption

Biometric data picked up by different devices must be protected and not be attached in clear to the subscribed document. One possible crook could, indeed, easily reuse them to create fake subscriptions on different documents. In order to solve this problem, all HS solutions envisage that biometric data, as soon as picked up, are encrypted with a strong encryption mechanism, before being included in or associated to the document being subscribed.

In case of litigation, data decryption is performed, upon request by the court, in order to assess one signature authenticity.

The reference scenario in such case envisages two steps:

1. One sequence of operations in order to decrypt the biometric data and to verify their integrity and their connection to the corresponding signed document;
2. Visualization of the previously decrypted biometric data and their analysis by graphology experts through one or more electronic tools.

There are several techniques too to issue encryption certificates and to manage the related private keys.

It also deserves being specified that the graphologist analysis as per step 2. implies the necessity of a comparison with additional signature samples or at least with samples of handwritten writings applied by the presumed signatory.

Such comparison can be performed between samples collected in different formats too, such as signatures applied on paper or HSs picked up with different tools or technologies, but for sure the appraisal is more effective if homogeneous specimens are available, picked up with the same technology and with analogous capture devices[3].

9.4) Interoperability set
In order to be able to proceed with the definition of the interoperability rules it is necessary to identify a unified data structure.

Such data structure should be legible with analysis tools provided by all producers that join this proposal of standardization, similarly, all biometric data encryption and extraction systems should generate such structure (either since it is natively adopted, or since it is obtained from converting proprietary formats).

Since the most relevant data are for sure the biometric ones and since an ISO/IEC standard exists, ISO/IEC 19794-7_2014 full format, there is no doubt that it is reasonable to opt for such a standard.

9. 5) ISO/IEC 19794-7 Biometric Data – Full Format
ISO/IEC 19794 standard defines a number of formats for exchanging biometric data, part 7 in particular is dedicated to representing temporal series of signature related data.

This standard allows for a representation at different detail levels and therefore arranges for a modular structure that describes measures varying in time deriving from a signature recording, the so called "channels".

For the purpose of a handwriting expertise, it is necessary to define a minimum set of data that are possibly always present.

9. 6) Minimum Requirements For ISO/IEC 19794-7_2014 Data
Hereinafter are defined the requirements for mandatory, recommended and optional channels among those envisaged by ISO/IEC 19794-7_2014.

[3] It is to be noted that "signature specimen" is referenced here, rather than "template" or centralised biometric data preservation. Since comparison is assigned to experts, not to automated recognition techniques, neither preliminary processing, nor centralised biometric data or signature characteristic features preservation is required. It suffices that the comparison samples are extracted from handwritten biometric signatures applied on different documents, which can be preserved with the same method as the documents subject to such analysis.

Non present channels (e.g. should channels F or S not be available) must be integrally omitted from the representation, without assigning a value to the corresponding description field in "channel inclusion field" (see section 8.3.2.8.1 of standard).

Mandatory data

X (in mm)

Y (in mm)

T or DT or equivalent heading information in case of constant frequency sampling

Recommended data

F (in N)

S (boolean)

Optional data

All other channels defined in ISO/IEC 19794-7_2014 standard are optional.

Recommended attributes for channels

ISO/IEC 19794-7_2014 standard envisages that all channel values are represented using a conversion allowing the two bytes range for the acquired biometric data (sample) (from 0 to 65536) depending on the measure accuracy.

For X and Y channels, maximum and minimum values should be indicated, additionally to the related scale range of values, in order to allow assessing both the actual physical size of the "signature gesture" on the screen, and its positioning in relation of the "signature box" (rectangle submitted onscreen to the user).

Chanel F should specify, in addition to the scale, also the minimum and maximum values as allowed by the device.

It is to be highlighted that gauging the system in Newton (N), albeit recommended, might be imprecise in several situations of signature capturing. On the other hand, even the ergonomic execution conditions (e.g. sitting at a table, standing at a counter, using a tablet device held with the other hand) can remarkably affect the pressure data absolute value. The latter has, therefore, mainly a "relative" value (or of trend) to be used jointly with other channels.

Time values can be expressed in any of the ways allowed by ISO/IEC 19794-7_2014: recording absolute time (T), difference with the preceding sampling (DT) or constant sampling frequency as indicated in the heading values.

Data Acquisition
All indications in ISO/IEC 19794-7_2014 Annex B are recommended for collecting signature samples having acceptable qualitative level.
In particular the following recommendations are highlighted.

Pixel Density
The minimum resolution value for channels X and Y should be of 4 points per mm (maximum variation: 5% per centimeter).

Sampling frequency
The sampling minum value should be 50 samples per second. There should not be a distance greater than 20 milliseconds between two samples with “pen in contact” (F>0 or S=1).

9.7) Signature Metadata

In order to correctly record all information related to the handwritten biometric signature capture technology, each solution should be able to produce, after having extracted the signature from the document, the following information:

- Capture device producer
- Capture device model
- Biometric data coding and enciphering software producer
- Software identifier
- Software version number

These metadata must be produced in XML format, consistently with a specific XSD schema.

9.8) Interoperability Proposal

These HS solutions interoperability proposal envisages that all producers joining this initiative prearrange an electronic tool suitable to extract signature data from the documents subscribed with their solutions.

Such tool, in addition to deciphering the protected data and to verifying the document integrity, should output two files for each extracted HS:

- An ISO/IEC 19794-7_2014 compliant file carrying the representation of channels in compliance with the minimum requirements as specified in the present document
- An XML metadata descriptive file abiding by the format defined in the present document.

Producers should provide this extraction tool to their customers, entitled to hold a HS solution, in particular this tool should be made available to third parties appointed to extract HS data from documents.

Producers of software solutions suitable for the expert analysis of signatures should instead integrate such format as input format to their products.

Obviously this format is applicable to the HS data in clear, i.e. in the format to be used solely under the trusted third party's control. Whenever it is to be transferred or exhibited, for example to court, the Trusted Third Party, that is responsible for its protection, shall necessarily resort to encryption.

The data structure and a recommended way to manage this kind of data structure is not defined in this document.

9.8.1 HS creation

From the above clauses stems the following basic procedure for the HS creation process.

As already said, a HS should meet these needs:

1) allow to assess the signed object integrity, e.g. to verify if the signed object's binary content has been modified in any way;
2) allow to assess the signed object authenticity, i.e. whether the purported subscriber is the actual subscriber.

In order to meet the integrity requirement as in previous item 1), two ways are possible:

a) adopt a purely HS solution;
b) adopt a mix of HS and Qualified Electronic Signature Solution; this in particular, would envisage affixing a QES (or, alternatively, a "qualified seal" as per the new EU Regulation 910/2014) to the HSed object.

In case a) the HS integrity could be verified only by enacting the HS Verification, that also allows to ascertain the HS authenticity, that would require to summon the purported signer and the decryption private key holder and activators.

In case b) the HSed object integrity could be checked at any time through the added QES, without summoning the purported signer and the decryption private key holder(s) and activators. The HSed object authenticity however could only be verified by implementing the HS signature verification.

Actual procedures enacted by the different HS creation solution existing in the marketplace usually differ from each other, however, the HS creation basic procedure should be as follows.

a) The signer affixes his/her HSs with a biometric signing device;
b) The signature channels and image are extracted by the signing device and securely sent to an application in a computer; if the computer is not the signing device itself (as in the case of a tablet as per clause 6.2) Biometric information collecting devices, item c) usually such device is connected to the computer via a secured USB connection;
c) The computer application, that has access to the to-be-signed document, applies a flow of hashing and encrypting functions to the received components: document, channels, signature image; The outcomes of the previous step can be combined to build the HS and to apply it to the to-be-signed document, that becomes a HSed document;
   where applicable, a final QES as per previous case B) can be affixed;
d) The HSed document is securely delivered or made available to the expected recipients: usually the signer(s), plus other possible recipients;
e) The HSed document is securely forwarded to a secure preservation system, where it is kept for the required time period.

All copies of channels in clear should be securely deleted as soon as they are no more necessary.

A core HS procedure as per previous item c) can be the following one.

Once the channels are securely received by the HS creation computer application, the latter should, for example, encrypt the channels, then concatenate the same channels in clear to the to-be-signed document and submit the resulting string to hashing. Both the encrypted channels and the digest resulting from the previously mentioned hashing, among other things, will be affixed or logically connected to the document.

The channels in clear would then be securely deleted. This would achieve the double goal of preventing a channels abuse and of meeting the EU Regulation 910/2014 requirement for AdES at art. 26, letter (d): "*it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.*"

Subsequent clause 10) Interoperability provides further details on the HS creation application, in particular on how the previously described two steps (encrypting the channels and hashing the concatenation of channels in clear and to-be-signed document) can be deemed as the HS Core component (see clause 10.1) Core HS).

Proprietary HS creation procedures can implement additional steps, for example in order to increase security by redundancy, but the above basic steps should be kept in order to facilitate interoperability.

Subsequent clause 9.8.2 HS verification will explain how the HSed integrity and authenticity can be verified.

> Note: Multiple HSs
>
> In some cases, e.g. when a contract is to be signed by two or more parties, one document would be HSed by more than one subscriber. In order to exhaustively verify all signatures (see clause 9.8.2 HS verification) all subscribers should be summoned to perform the required verification procedure. This nuisance can be partly worked around, and not only in relation to the HSed object integrity, if a trusted third party (e.g. a Notary, in the case where the document submitted to HS is a contract drawn and signed in presence of the same Notary) applies a QES at the end that endorses also a Notary's assertion stating that all attending persons have applied their HS to the document.
>
> This would allow any document reader to quickly verify the Notary's QESs and therefore to ascertain the HSed document overall integrity.

9.8.2 HS verification

A complete HS verification allows to verify both the signature authenticity, i.e. if the purported subscriber(s) is(are) the presumed one(s), and its integrity, i.e. if the document has changed after the signature.

As the HS integrity is concerned the following two cases can apply:

a) If a final QES was affixed as per clause 9.8.1 HS creation, item B), the HS integrity could be verified at any time by verifying such final QES, but the authenticity would not be ascertained;
b) If such final QES was not applied, then in order to verify the HSed object integrity the complete HS verification process is to be applied. This would also ascertain the signed object authenticity as below specified.

In order to verify the HSed document authenticity, i.e. to ascertain if the purported subscriber(s) was (were) the actual signer(s), the complete HS verification process is always to be performed. Such process depends on the HS creation procedure . In particular the HS verification basic procedure should be the following.

a) The private decryption key holder and the persons entitled to activate it join together (at least virtually) and the key is activated;
b) The HS is logically extracted from the signed document and its parts, encrypted as described in clause 9.8.1 HS creation, are decrypted;
c) The document integrity is verified as follows, for example. The decrypted channels could be concatenated with the document, the outcome being hashed and the resulting digest being checked against the digest contained in the HS; if the integrity appears as violated the verification process should stop;
d) The purported signer, where present, is requested to apply a number of HSs on a suitable device; from the channels of these signature a template can be built;
e) A graphologist verifies if the channels just decrypted from the HSed document are compatible with the template.

Once the verification process is over, all channels in clear are securely deleted.

Obviously the described process is just a basic, raw, flow that can be revised and integrated by the standardisation bodies.

Where proprietary HS creation procedures have implemented additional steps, for example in order to increase security by redundancy, these additional steps should be verified as well, but, if the HS creation had, among its steps, implemented the raw procedure as in clause 9.8.1 HS creation, the verification above applies and should suffice.

10) Interoperability

As previously hinted to, it can be assumed that every single HS creation/verification solution is in principle proprietary, i.e. different from the other ones, therefore migrating from one solution to another could imply great difficulty, if not outright impossibility, in verifying HS created with the previous solution. As a consequence, one organisation that began providing its users with one HS solution would be bound forever to that solution, hence and possibly to its provider.

It is therefore a need, in order to meet the EU requirement on a free market, to design a standard HS creation and verification procedure as well as a HS structure, which implies defining the structure of each single HS component, that, once implemented, would allow organisations a free moving between providers.

Defining such procedure is left up to the suitable standardisation body, but it seems reasonable that the basic HS creation and verification procedures described at clauses 9.8.1 HS creation and 9.8.2 HS verification can be a good starting point.

One possible solution to achieve interoperability could be to define a "Core HS" and a set of "HS Extensions". The structure of both "Core HS" and "HS Extensions" should be defined by a standard and they should also be assigned unique codes, in order to allow any verifier to identify each single component and choose which one to verify, in addition to the Core HS ones.

10.1) Core HS

The Core HS could be built, for example, on the two previously said components:

a) Encrypted channels
b) Digest resulting from the hash of the concatenation of the channels and the to-be-signed document.

These two components should be given a unique identifier and clearly structured so to make their verification univocally possible.

Verifying a HS that holds these two components would univocally assure its integrity and authenticity.

10.2) HS Extensions

In addition to the Core HS it has already been discussed that a QES can optionally be affixed to the HSed object as the signature final step, in order to make it possible to easily verify the HS integrity at any moment without much hassle.

Further extensions can be applied by the various HS solutions developers, for example in order to enhance the HS security through "security by redundancy". Just to make an example, one developer may want to enhance the HS robustness by hashing the encrypted channels, in order to build an additional obstacle to tampering.

Each of these components should be given a unique identifier and clearly structured so to make it possible, in verification phase, to identify each of them and to univocally verify it.

10.3) Reliable Interoperability

As far as Interoperability is concerned, four solutions could be envisaged.

a) "High" level solutions

1) The previously mentioned solution of adopting one common process for both creation of a HS and for its verification;
   The advantage of this solution are all too apparent;
2) Additionally, it could be envisaged to separate generation and verification process, in a way that any HS generation process, regardless of how it is implemented, creates one common HS format; in this case only the verification process should be standardised;
   The advantage of this solution would be that each HS solution developer might keep its HS generation somewhat confidential, while allowing for a verification process interoperability;

b) "Substantial" level solutions

HS solution developers:

1) would develop a verification ("unpacking") tool too, to be distributed to their client organisations (i.e. not to single subscribers), either free or fee;
2) would publish the verification ("unpacking") technical specifications, so that their client organisations could implement by themselves the related software application.

Note: Security considerations

Case a) would be the most reliable one, since the "unpacking" Software would be used by the client organization while it is still under the HS solution producer, which would provide better reliance upon the producer.

Case b) would be still reliable enough, albeit solution b)1) would be even more reliable if such tool is provided by the producer to its client organisations when they are still under its control.

Solution b) 2) would benefit from the possibility to inspect the lines of code, possibly identifying possible malware.

Finally, Case b) solutions could benefit from more reliability if tools and SW specifications were certified ISO/IEC 15408, at least Level EAL 2, but this might imply a remarkable cost.

11) Security Measures

All components and steps in a HS creation and verification procedure should be secured, in order to prevent at least:

1) Channels misuse, that could imply even their abusive apposition to documents the original signer is unaware of;
2) Tampering with the signed document, without this tampering being recognised, thus violating requirement in EU Regulation 910/2014, art. 26, letter (d): "*An advanced electronic signature … is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.*"

<u>In HS creation phase</u>

In principle, among all components of a HS creation procedure, at least the following ones would require suitable security measures.

a) Biometric device with which the HS is affixed and that extracts the related channels;
   the security measures purpose would be to prevent channels from being captured or altered by fraudulent applications;
b) Link between the device above and the computer to which it is connected; as anticipated in clause 6.2) Biometric information collecting devices, item c), the case where the channels collecting device is a general purpose tablet should also be specifically addressed;
   the security measures purpose would be to prevent channels from being captured or altered by fraudulent applications;
c) Computer where the HS creation application resides;

the security measures purpose would be to prevent all HS creation steps from being intruded by fraudulent applications in order to capture or alter channels, HS components etc.;

d) Encryption key, to assure using organisations that it actually corresponds to the decryption key held by the appointed trusted entity;
the security measures purpose would be to prevent altering the encryption key;

e) Connection between the computer where the HS creation application resides and the secure preservation system where the HSed document is to be archived;
the security measures purpose would be in this case double:
    1) to prevent "officially" HSed objects from being captured and/or tampered with by fraudulent applications;
    2) to prevent fake HSed objects from being fraudulently added to the "official" secure preservation system;

f) Secure preservation system – as far as this system is concerned, ETSI TS 101 533-01 lays down security measures suitable to ensure long term secure preservation preventing alteration, deletion, insertion;
the security measures purpose would be to prevent capturing of and tampering with the preserved documents, as well as to prevent inserting fraudulent objects.

Note: although it may seem unreasonable or unnecessary, preventing "insertion" is indispensable as well, as hinted to in clause 6.4) HSed documents preservation, because it would prevent insertion of fake HSed objects into the archive; it is worth reminding that preservation in a secure archive is a basic issue of the authenticity verification.

In HS verification phase

In principle, among all components of a HS verification procedure, at least the following ones would require suitable security measures.

A) A suitable device as in previous item a);
B) The same link as in previous item b);
C) Computer where the HS verification procedure resides;
the security measures purpose would be to prevent all HS creation steps from being intruded by fraudulent applications in order to capture or alter channels, HS components etc.;

D) Connection between the secure preservation system where the HSed document to be verified is archived (see previous item f)) and the computer where the HS verification application resides;
the security measures purpose would be:
   a. to prevent "officially" HSed objects from being captured and/or tampered with by fraudulent applications when in transit;
   b. to prevent fake HSed objects from being fraudulently added to the verification phase, masquerading them as "authentic" HSed objects;

E) Decryption key, both in order to protect it from attacks and to ensure a reliable access;
the security measures purpose would be to prevent tampering and capture both of the "active" private key and of its backup copies;
Note: among the security measures related to the decryption key, it would also be worth envisaging that its activation password is divided in "m" parts in a way that "n" of such "m" parts are enough to activate the key. Obviously each of the "m" parts should be securely kept by different persons and "n" should be equal or greater than two;

F) Tools used by the graphologist who assesses the compatibility of the decrypted channels with the template built on the signatures affixed by the purported signer at verification phase on devices as in item A);
the security measures purpose would be:
   a. to prevent used channels from being captured and/or tampered with by fraudulent applications;
   b. to prevent fake channels from being fraudulently added to the verification procedure, to masquerade them as belonging to a HS under verification.

12) Document formats

All documents to which an AdES format is applied should be drafted in formats unsuitable to host Presentation Corruption Agents – PCA[4]. Among formats that are inherently unsuitable to host PCA, the following can be listed, thus these formats should be recommended to be used:

[4] A PCA is a kind of malware capable to modify a digital object presentation to a human eye without affecting the binary content of the hosting digital object. Examples of PCA can be macros and hidden code.

1) PDF/A – this format, in fact, does neither fetch any information from the outside, nor host macroinstructions;
2) TXT – this format, providing a "plain" presentation of its binary content, cannot host PCA.

XML can also be used, provided that the following requirements are met by the XML object:

a) It should refer to a scheme that either is internal to the XML, or is fetched from a trusted source and its integrity and authenticity are ensured, for instance via a QES issued by a trusted entity;
b) It fetches no information from outside, or at least such information is fetched from trusted sources and its integrity and authenticity are ensured, for instance via a QES issued by a trusted entity.

No other general purpose formats enjoy such PCA prevention. However, in specific cases, other formats can be used when the involved persons are reasonably confident that the to-be-signed document is free from any PCA.

The standardisation bodies should clearly define which format(s) can be used with a HS and in which context. Hereinafter some suggestions are provided

1) High Security – in order to actually *prevent* PCAs to be hosted in one document, the previously listed document formats should be used;
2) Substantial security – where is it deemed sufficient for the process not to absolutely prevent PCAs from being added to one document to be signed, but to provide the reader with a warning that the presentation has been altered, then plain PDF format would suffice. In fact, in addition to the changing to the document binary content, that is under the scrutiny of a signature, PDF per se, when opening a document, verifies if its original presentation has changed, and in case it provides a suitable warning.
   No other document format provides such inspection and consequent warning. Another issue is to be taken into account, though: one subscriber, who is compelled to draft and sign a PDF document he/she is not willing to endorse, might introduce a PCA into this document that would modify its presentation. When the document is opened the previously mentioned warning would appear. This way the document he / she was not willing to subscribe would be nullified, thus meeting the subscriber's intention.

Additionally, in the PDF/A case, it is reasonable to envisage a new PAdES format suitable to host a HS.

13) Bibliography

This clause lists documents, in addition to those listed in clause 3) Reference, that provide information suitable to better understand the HS environment.

13.1) Legislative bibliography

1) Dlgs 82/2005 - Codice dell'amministrazione digitale – Decreto legislativo 7 marzo 2005, n. 82
2) DPCM 22/2/2013 – DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71 del Dlgs 82/2005
3) DPCM 3/12/2013 - DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 – Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
4) PROVVEDIMENTO del Garante dei dati personali n. 513/2014 del 12 novembre 2014 - Provvedimento generale prescrittivo in tema di biometria
5) Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL os 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

13.2) Technical bibliography and sitography

a) Roud Bolle et alii, Guide to Biometrics, Springer, 2004
b) www.aifag.it