

New World Order – The Case for the Galaxkey Trusted Digital Document Signing



www.galaxkey.com

The Case for the Galaxkey Trusted Digital Document Signing



The distanced, out of office (off campus) operational dictates of the 2020 pandemic have imposed the requirement to evolve and deliver New Age Working Practices (NAWP) to sustain secure, assured operability and communication in support of the business mission. However, in this impasse of criminal opportunity, hackers, organised criminals and even state sponsored actors have sought to leverage the enhanced surface of attack presented by multiples of international companies. In some cases, manifesting in social engineering to persuade the transfer of multi-million £/\$ transactions into illicit accounts through the use of manipulated communications; or the uttering/presentation of falsified documents to lure the recipient into believing what they are reading is the truth – all of which create a real-world, everyday security trust vulnerability for users and their companies alike.

By example, one such case of the abuse of trust, and the lack of assured provenance of a document security is that of the leaked document used by an MP as proof that the Conservative Party were planning to sell off the NHS – documents which have now been discredited, and linked to a Russian disinformation campaign of “Secondary Infektion”, uncovered by Facebook in 2020. Here there is a very strong argument in favour of assuring document provenance and trust with solutions such as Galaxkeys Digital Signing system to robustly secure an object in the electronic form.

It is also worthy of note that on 21/07/20 the Intelligence and Security Committee of the UK Parliament published their paper on the threat posed by Russia, which outlined the Russians and their circulation of disinformation. It is here, where again we see a very strong case for document and security.

In this imposed NAWP there is a clear business need to:

- a. Accommodate Systems that enhance the level of ‘Trust’**
- b. Provide Mechanisms which are, as far as practicable beyond reproach**
- c. Deliver solutions that may be employed enterprise wide**
- d. Accommodate facilities to encompass Out-of-Band (OoB) organizations**
- e. Underpin mandated Policies, Standards and Legal Expectations**



The Case for the Galaxkey Trusted Digital Document Signing

Solution

One obvious solution is to deploy an assured and trusted methodology which provides an additional level of assurance that the object in view is a single qualified representation of the truth, is genuine, and thus can be trusted. Clearly, when it comes to a Face-2-Face (F2F) commercial negotiation, with one party signing a document in presence of the other, with the attendance of witnesses is of course considered a trusted, none-refutable transaction. However, with a communication that is distance based, or one which has evolved as a product of NAWP, in pure pragmatic terms businesses must evolve a trusted operational capability to promote and support 'Trust'. Here one very solid solution is that of Digitally Signing a document to support the objects provenance and trustworthiness. However, I am aware from many discussions that there are questions and confusions within organisations when such solutions are considered, and so in this independent paper I seek to address some of the main concerns and observations in a positive way.


The Legal Position

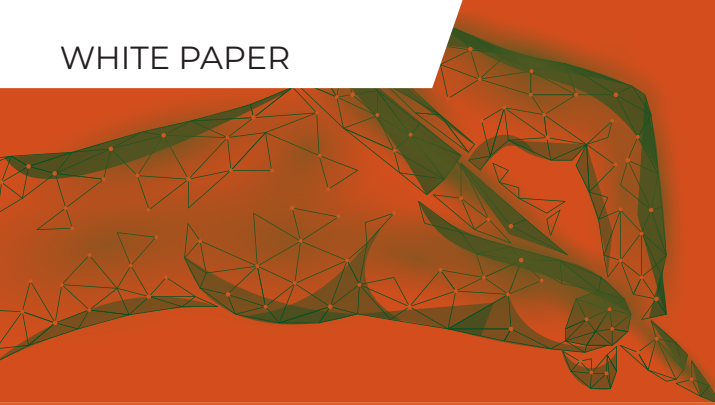
In the wider context, and to address the some of the major concerns around Digital Signing of a Document and the associated legal implications relating to trust, one may look to the legislations around Digital Signatures covered by consultations in 2018 of the Law Commission in England and Wales who issued their report in September 2019 (the "**Commission's Report**") clarifying the legal validity of the use of the electronic signature to execute a valid contract. They concluded that the different forms of electronic signature can be divided into three groups:

-  **Simple electronic signatures** - these are scanned signatures or a tick-box plus declaration.
-  **Advanced electronic signatures** - these can identify the user, are unique to them, are under the sole control of the user and are attached to a document in a way that it becomes invalidated if the contents are changed (e.g. Galaxkey);

-  **Qualified electronic signatures** - these are advanced electronic signatures with a digital certificate encrypted by way of a secure signature creation device (Galaxkey Platform) e.g. smart card

Considering the legislative provisions on electronic documents and signatures, Scots and English law have their basis in European law. Regulation (EU) No 910/2014 (the "eIDAS Regulation"), which replaces EU Directive 1999/93/EC. This has driven the direct effect in EU Member States from 1st July 2016 and establishes an EU-wide legal framework for electronic signatures. The eIDAS Regulation defines:

-  An "electronic signature" as "data in electronic form which is attached to or logically associated with other data in electronic form (say a document) and which is used by the signatory to sign"



The Case for the Galaxkey Trusted Digital Document Signing

- 🔒 An “advanced electronic signature” as one which meets the following requirements: (i) it is uniquely linked to the signatory; (ii) it is capable of identifying the signatory; (iii) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (iv) it is linked to the data (document) signed therewith in such a way that any subsequent change in the data is detectable; and
- 🔒 A “qualified electronic signature” as “an advanced electronic signature that is created by a qualified electronic signature creation device (Galaxkey Platform), and which is based on a qualified certificate for electronic signatures”

Note 1

Galaxkey meet all expectations of the above security objectives

As a further example, The Land Registration - (Scotland) Act 2012 and the Electronic Documents (Scotland) Regulations 2014 now confer the same status and standards of validity on documents created in electronic form to those given in the form of hard-copy paper documents

Note 2

The exception here is, wills and testamentary writings which must be created and signed in traditional form (for the meantime).

In reviewing other relevant legal provisions, a Joint Working Party comprising The Law Society, Company Law Committee, The City of London Law Society Company Law and Financial Law Committees (“the JWP”) formed the opinion that a contract executed using an electronic signature (and which may be signed solely in electronic form) satisfies a statutory requirement to be in writing and/or signed and/or under hand. This position may be asserted to extend to that of a Digitally Signed Document. However, this paper both recognises and acknowledges that to accomplish and

complete end-to-end assured, trusted solution the deployment must not only focus on technology, but must encompass the related practices that accommodate provisioning of a complete trusted solution – this will be covered later by this paper.

We should also consider some other verticals, such as, and by example that of the US Life Sciences Regulations (21 CFR Part II) which impose additional requirements beyond those of the general U.S. laws regarding eSignatures and digital transactions. For example, 21 CFR Part 11 which outlines the requirements for

The Case for the Galaxkey Trusted Digital Document Signing

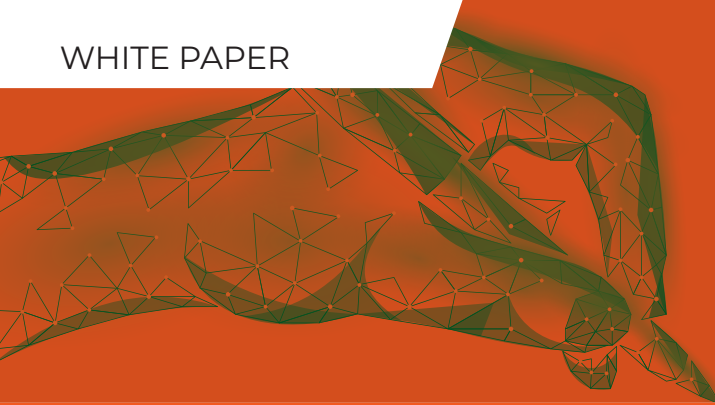
electronic records and electronic signatures to be accepted by the FDA. Among other things, Part 11 requires that electronic records:

- 🔒 Be validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern valid or altered records
- 🔒 Be able to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the FDA
- 🔒 Ensure records are protected
- 🔒 Limit access to authorized individuals
- 🔒 Use secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records

At the International level, one must always consider the local rules of the particular domicile when deploying any technology, but overall, the purpose of this paper is to provide a level of assurance that, given correct implementation, deployment and support, such a service as provided by Galaxkey may be considered a trusted operational solution to assure robust document provenance, integrity and trustworthiness are fully accommodated.

Note 3

As part of the research behind this paper, the author interviewed a selection of high-end UK legal practices to seek their opinion as to document signing, and electronic signatures. These interviews firmly concluded that, albeit the findings were agnostic to the employed technical solutions, document signing and digital signatures, are used and trusted as common practice to secure communicated and distributed electronic objects.



The Case for the Galaxkey Trusted Digital Document Signing

Assured Processes

Of course, it is not just about simply installing an application and forgetting it. When we look to deploy the concept of a trusted security solutions such as eSignatures, or Document Signing, it is of paramount importance that what is being secured is accurate, true, and maintained to underpin the overall security objective. It is here where the Galaxkey solution(s) go one step further and are working to underpin additional assured levels of company/user provisioning to elevate the level of associated trust to a higher level than many of their competitors employ. Galaxkey are also partnering with Yoti who provide a tethered user identification solution tied into 'something you have' credentials, such as a valid driving licence, or UK passport which are fully qualified by Yoti prior to them being accepted (trusted) and thus by implication, enhances the level of trust of the Galaxkey solution to a higher robust level.

Supporting Policies

As outlined above, to achieve a fully qualified robust service it is of paramount importance that the technology is underpinned with direction of secure operability. In the case of the Galaxkey Document Signing methodology they are working to provision their client user base with a top-level generic policy template to support their applications in the live operational setting to ensure it is employed to meet the best security working practices to maximize the level of security operability.

Training and User Support

As outlined above, to deploy a robust solution, especially in the form of a Document Signing application, and to assure it's robustness goes well beyond the technical level, it is here where Galaxkey again go the extra mile, when compared to their rivals. Galaxkey are evolving a set Security Education and Awareness tools to educate the product user base of best practices which need to be applied – again taking the product beyond just a technological solution to a fully fledged end-to-end managed secure set of component(s).



The Case for the Galaxkey Trusted Digital Document Signing

Government Certification

Given that Galaxkey have gone through the rigour of CPA (Commercial Product Assurance) under the UK National Cyber Security Centre (NCSC) scheme and achieved Certification of their email platform, they may be asserted to be a robust and trusted provider with a proven, independently verified assured platform to meet the requirements of NAWP – See NCSC associated link below:

<https://www.ncsc.gov.uk/products/galaxkey>

Platforms

In the current Cyber Security climate there is fear and doubt of the current threats posed by International State Sponsored Actors and Criminals. To address this, Galaxkey systems are either hosted in the UK, or by user election, deployed internal to their own on-campus operational facilities – reducing/mitigating the potential threat of adverse actors manipulating the systems and components to which they have potential ease of access. Furthermore, Galaxkey are a UK based/owned company with no development association with any known international bad actors such as China or Russia.

End-to-End Secure Solution

Taking into account the wide range of services Galaxkey offer complimentary to Digital Signing and Document Management solutions, it is clear that they go well beyond their closest rivals to achieve a complete end-to-end robust lifecycle to manage communications, and document security. Ranging from Document Classification, Secure Email, Secure Collaboration, Cloud Synchronization and GDPR support. One other major added benefit of using Galaxkey is the user organisation are dealing with one company to achieve multiple integrated security expectations, which not only reduce the implications of the process of patch fix and update, but also provide an assurance of product compatibility and stability.

The Case for the Galaxkey Trusted Digital Document Signing

Conclusion

In conclusion, the case for deployment of Document Digital Signing technologies is strong in both legal, and operational security terms. For companies seeking to secure their NAWP business interests and sensitive information assets, such mechanisms should be asserted to be a must have security technology to inbuild into their cyber defence capabilities - provisioning robust assurance and provenance for documents they produce, and distribute. It is clear the benefits of document signing are a highly effective underpin of security, trust, and legally acceptability that are asserted to exist within a professional, operational world driven by technology and electronic commercial business transactions.

Furthermore, whilst there are multiple solutions available to support such secure business operability, having evaluated and used the Galaxkey solution(s) they were proven to provision an overall conjoined one-stop-shop set of solutions to accommodate robust digital document signing and document management which meet the enhanced security expectations of the Secure Electronic Document Lifecycle, and mandated Standards as outlined in this paper. Observations which are further supported by a set of multi-faceted security features, along with the association of independently verified UK Government Security Certification. Galaxkey certainly represent a trusted single-source of interconnected security platforms which offer multiples of associated, complimentary support of document management, collaboration, secure distribution, and of course digital document signing., The Galaxkey approach also removes the complexity of integration of multiple components to achieve the various levels of anticipated secure operability. Here further benefits may be had by reducing the every-day potential of multi-system patch, fix, and update to achieve a fully maintained compatible platforms under one integrated set related applications.

Returning to the introduction of this paper, and mindful of the cyber threats now faced by multiples of international organisations, along with the known-known associated successful security attacks, compromises, disinformation and social engineering by electronic means, we must sadly accept the threat is ever present and growing in pure Active Persistent Threat (APT) terms. Thus, the ultimate final bottom line conclusion must be, the case for securing organisational digital assets by employment of a legally acceptable digital document signing methodology has never been stronger.

*Professor John Walker
24 July 2020
Independent Cyber Security Professional*