Bird & Bird

Bird & Bird
Advokatpartnerselskab
Kalkbraenderiloebskaj 4
2100 Copenhagen
Denmark
Europaplads 2
8000 Aarhus C
Denmark
Tel +45 72 24 12 12
Fax +45 72 24 12 13
twobirds.com

MEMORANDUM

To:	Signicat AS
From:	Nis Dall
Date:	6 December 2016
Client:	Signicat AS
Subject:	Signicat Signature in relation to eIDAS
Matter No:	SIGAS.0001

1. INTRODUCTION

Signicat AS (hereinafter referred to as "Signicat") has asked Bird & Bird to assess two overall matters in relation to their product Signicat Signature and the eIDAS-regulation (hereinafter referred to as "eIDAS").

Signicat wish for the following to be assessed:

1. Does Signicat Signature fulfil the requirements to be an 'advanced' electronic signature in relation to eIDAS?

2. Is it necessary to use an 'advanced' signature in order for the signature to be accepted as proof in legal proceedings?

1.1 Generally on Signicat Signature

Signicat Signature is a system where Signicat provides an electronic signature based on another electronic identification system.

This means that when Signicat Signature is used, the signatory authenticates him-/her-self through the use of another electronic identification system (hereinafter referred to as an "eID"), e.g. NemID in Denmark or BankID in Norway.

The document is then signed/approved by the signatory and sealed by Signicat leading to a "package" containing proof of identification and the signed document.

Thus, use of Signicat Signature means that the business providing the electronic document for signing can accept a number of different eIDs in the same context, depending on which eID is available to the signatory.

1.2 Generally on the eIDAS

eIDAS, or the Regulation on electronic identification and trust services for electronic transactions in the internal market, which has become effective in the EU on 1 July 2016 and replaces the earlier directive on electronic signatures.

The Regulation is as such technology neutral which is important when introducing new technology in relation to electronic identification and signatures, but sets up requirements for electronic signatures, electronic seals etc.

The Regulation apply to a) Electronic identification schemes that have been notified [to the Commission] by a Member State, and b) Trust service providers that are established in the Union.

2. THE STATUS OF SIGNICAT SIGNATURE UNDER EIDAS?

2.1 Electronic signature

An electronic signature is defined in the eIDAS as:

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

This is a very broad definition and covers even electronic handwritten signatures made with e.g. a Stylus or the like.

The requirements are indisputably fulfilled by the Signicat Signature since it is data in electronic form; the electronic data is attached to other data, i.e. the document in the 'package', and the data in electronic form is being used by the signatory to sign the document in question.

2.2 Advanced electronic signature

In order to be an advanced electronic signature, the electronic signature needs to further comply with the following:

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

Both requirements a) and b), i.e. the requirements on the advanced electronic signature being uniquely linked to the signatory and being capable to identify the signatory, depend on the eID being used by the signatory in relation to Signicat Signature.

The 'package' produced with Signicat Signature contains proof of identification and the signed document and hence links the two. But the *proof of identification* contained in the package is a proof of which eID has been used by the signatory, and hence this relation depends on the eID.

If the eID being used is uniquely linked to and identifies the signatory, then requirements a) and b) will be fulfilled when using Signicat Signature.

In relation to requirement c), the signature creation data, when making use of Signicat Signature, is the eID being used by the signatory which - at least in relation to Signicat Signature – is under the sole control of the signatory – the fulfilment of requirement c) also depends on the eID being used. If the eID provides a high level of confidence of the electronic signature creation data being under the sole control of the signatory, then this requirement will be fulfilled in relation to Signicat Signature.

Regarding requirement (d); Linkage between the electronic signature and the signed document in a tamper-proof way is in the Signicat Signature solution ensured through packaging both proof of identification and the document and then sealing the package.

The seal used in Signicat Signature is, as far as we understand, tamper-proof as it makes use of a combined hashing of both proof of identity and the signed document based on XAdES.

Based on the above, in the opinion of Bird & Bird, the Signicat Signature solution can provide for advanced electronic signatures, provided though that the eID being used by the signatory within Signicat Signature fulfils requirements a)-c) above.

3. PROOF IN LEGAL PROCEEDINGS?

3.1 Overall non-discrimination

The eIDAS regulations set up principles for recognition of electronic signatures in legal proceedings in the EU.

The first principle is that an electronic signature shall not be denied legal effect and admissibility in legal proceedings, due to the fact that the signature is in electronic form or due to the electronic signature not being a qualified electronic signature.

This means that all electronic signatures shall be recognised and be admitted as (part of) a proof in legal proceedings in all of the EU.

It is, however, a matter of national law in each of the EU member states to decide which legal effect, i.e. value as proof, such electronic signatures shall have in legal proceedings.

Only in relation to qualified electronic signatures, the eIDAS sets a specific value, namely that qualified electronic signatures shall have the same legal effect as a handwritten signature in each member state. But it should be noted that even the value of a handwritten signature in legal proceedings vary from member state to member state, e.g. a number of member states require certain documents to be notified by a notary, even when appropriately signed.

Hence, for all electronic signatures – which as mentioned above – is a very broad definition, it is fully up to the legal systems of each member state to set a 'proof-value' to electronic signatures.

Therefore, it is not required for an electronic signature to be of the advanced type in relation to the electronic signature to be presented as proof in legal proceedings

anywhere in the EU. Due to the requirements placed on advanced electronic signatures, fulfilling these will, however, raise the value as proof.

3.2 Denmark

3.2.1 General principle of free evaluation of proof

In civil procedural rules in Denmark, the value of a certain piece of proof, e.g. a signed document, is to be freely evaluated by the court.

The use of electronic signatures will be accepted in Danish courts – which is now also a requirement of eIDAS. The value of the proof may, however, vary from case to case.

Where a party denies ever having entered into the agreement, this can usually happen in one of two ways, i.e. the party either denies that the document is signed or that the party is not the signatory.

In such situations, having made use of an advanced electronic signature would be beneficial since, due to the characteristics of the advanced electronic signature, it would entail a) a unique link to the signatory, b) identification of the signatory and that c) the signature would – to a high degree of confidence – have been under the sole control of the (given) signatory.

This would create such an assumption that only the given signatory could in fact have signed the document which d) is linked to the signature that it would be up to the signatory to introduce proof that it was in fact not him which had signed the document – a burden of proof which would be hard to satisfy, except in very rare cases.

As mentioned above in section 2.2, the value of the advanced electronic signature as proof – and even if the electronic signature is in fact advanced or not – would in relation to a)-c) be based on the eID having been used for the signature. The higher the requirements in relation to the eID used – the eIDAS operates with assurance levels of eIDs being either low, substantial or high – the more non-repudiable the advanced electronic signature would be as proof.

3.2.2 Enforcement

In Denmark, previously, there have been requirements in the Administration of Justice Act making it impossible, or at least difficult, to enforce electronically signed documents without having first obtained a court ruling.

However, changes in the Administration of Justice Act have made such enforcement easier. These changes have led to a) out-of-court settlements and promissory notes, which state that they can be enforced without having obtained a court order and which have been signed electronically, are now enforceable directly in the Bailiff's court. The same is the case with b) credit purchase agreements containing a statement of retention of title and which

are electronically signed, in which case a retention can be enforced through the Bailiff's court.

It is not stated in the Administration of Justice Act that the electronical signature, used in relation to the document which is now to be enforced, is to be of a certain type. However, based on the preparatory work for the change in the Administration of Justice Act, the requirement in relation to the electronical signature used is that it should be based on the so-called OCES-standard, or with a security level equivalent thereto. OCES is a Danish standard (Offentlige Certifikater til Elektronisk Service) and is the basis for the Danish NemID.

The intention in the preparatory work most likely was to state that signatures, which were to be accepted for making documents enforceable directly in the Bailiff's court, were to be advanced electronical signatures.

If Signicat Signature is based on a NemID-eID, the requirement would be fulfilled since the security would be as/equivalent to the NemID-signatures and hence with the security level of OCES. This could also be the case when using other eIDs than NemID, but this must be evaluated on an eID by eID basis.

Further, previously, it was required that the *original* document was presented in the Bailiff's court which was interpreted as the document with the handwritten signature. This has also been changed in relation to out-of-court settlements and promissory notes, meaning that when enforcing such documents, a written representation of the document must be presented in the Bailiff's court. Such representation of the document shall be an exact representation of the document having been electronically signed by the signatory.

If an objection on the contents of the representation of the signed document is made, it will be up to the party claiming that the representation is correct to show this. I.e. by forwarding documentation on the tamper-proof attributes of the electronic signature used. There is, however, a risk that such objection would make the Bailiff's court refuse the enforcement, making it necessary for the claimant to obtain a 'normal' court ruling. This is due to the Bailiff's court not being required to obtain substantial evidence in enforcement matters.

3.3 Norway

3.3.1 General principle of free evaluation of proof

In Norway, the principle of free evaluation of proof applies, thus the value of a signed document or any other evidence is to be freely evaluated by the court.

The use of electronic signatures will be accepted in Norwegian courts, but the assessment of whether the signature is valid and can be enforced depends on the courts' free evaluation. The validity of an electronic signature will thus vary from case to case.

When a party denies having entered into an agreement, this is typically based on one of two allegations, 1) that the party denies that the document is signed or 2) that the party is not the signatory. In such situations, it would also in Norway as in Denmark, be a benefit to have used an advanced electronic signature. This is due to the characteristics of an advanced electronic signature, which in Norway corresponds with the Danish definition of advanced signature. It would entail a) a unique link to the signatory, b) identification of the signatory and c) that the signature would – to a high degree of confidence – have been under the sole control of the (given) signatory. This would create such an assumption that only the given signatory could in fact have signed the document which is linked to the signature. It would be up to the signatory to present proof that it was in fact still someone else who had signed the document – a burden of proof which would be hard to satisfy, except in very rare cases.

As mentioned above in relation to Denmark; the value of an advanced electronic signature as proof would in relation to a)-c) would be based on the eID having been used for the signature. The higher the requirements in relation to the eID used – the eIDAS operates with assurance levels of eIDs being either low, substantial or high – the more non-reputable the advanced electronic signature would be as proof.

3.3.2 Enforcement

The eIDAS has, at present, not been implemented in Norway. However, when the eIDAS regulation is made a part of the EEA agreement, Norway will follow suit and implement the regulation with very few changes. The eIDAS is expected to be included in the EEA agreement in February 2017.

The implementation of eIDAS does not change the overall current legal status of e-signatures, regulated by the Norwegian E-signature Act (No 81 of 2001). According to the act, electronic signatures could be considered on equal footing as a handwritten signature. However, the enforcement of an electronic signature will still depend, in many cases, on the courts' evaluation.

Currently, electronic signatures are not considered valid for enforcement of instruments of debt. According to the Supreme Court's interpretation of the Norwegian Legal Enforcement Act (NO 86 of 1992), electronic signatures are not considered sufficient to enforce an instrument of debt without first obtaining a court order. Thus at present there have not been implemented any changes in Norway corresponding to the Danish Administration of Justice Act opening up for the use of electronic signatures. In Norway, the original document with the handwritten signature is still the only enforceable document.

However, the preparatory acts for the Norwegian implementation of eIDAS indicate that the implementation of this regulation will lead to similar changes in the Norwegian Act of Legal Enforcement as well as other related laws, thus making electronic signatures a valid and enforceable signature. The exact scope and content of these changes have yet to be finally decided and communicated.

3.4 Sweden

3.4.1 Legal effects of signatures in general

Under Swedish private law, there are relatively few rules requiring a signature in order for a certain legal consequence to take effect, e.g. for a certain agreement to be valid and enforceable. This is in contrast to administrative law, where signature and written form requirements are more common, e.g. when submitting applications to Swedish authorities. In business practice, signatures constitute an established method of confirming, controlling and proving business actions of contracting parties.

Even though, in light of the above, in most business transactions a signature may not be required by law, it still can have evidentiary value.

In this context, it should be noted that an act of denying to sign a certain document may be criminalised (with a fine or imprisonment for up to six months), provided that such an act jeopardises evidence (Sw. fara i bevishänseende). Since 2013, this criminal sanction also applies to an act of denying signing an electronic document if the certificate of such document may be reliably controlled.

3.4.2 Legal effect of electronic signatures in particular

As far as electronic signatures are concerned, there are no specific rules which would in general restrict or deny electronic signatures legal effect.

The legislator has deemed electronic signatures of high quality to be at least as secure as traditional, hand-written signatures. However, it has not been considered appropriate to introduce a general rule that gives electronic signatures the same legal value as handwritten signatures.

From the now abolished Act on Qualified Electronic Signatures (2000:832)(the "Signature Act") followed as a main rule that if any other law required a handwritten signature, a qualified electronic signature would be deemed to fulfil such a requirement, provided that such law did not explicitly prohibit electronic signatures.

Pursuant to the eIDAS regulation, it is now clarified that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

3.4.3 Free evaluation of evidence

Under civil procedural law, the principle of free evaluation of evidence applies. This means that all types of evidence are permitted and judges are free to assess and evaluate the evidentiary value of adduced evidence.

Consequently, electronic signatures are admissible as evidence in Swedish courts, which now also follows explicitly from eIDAS regulation.

The government has hitherto declared that there is no need for special evidentiary rules concerning electronic signatures.

Swedish case law does not present uniform and consistent procedural principles, where one party objects that a signature, irrespective of whether it is a hand-written or electronic one, has been forged. However, in light of relatively recent case law (2011-2012) the burden of proof, with a low evidentiary requirement, would most likely be placed with the debtor. This means that a debtor would need to prove that a signature has been forged, e.g. submit evidence that supports this statement.

It should be noted that under Swedish procedural law, the burden of proof is often placed with the party that is best suited to secure and preserve evidence. In this case, i.e. where a debtor claims that their signature has been forged, it has been contested whether a debtor or creditor ought to prove whether a contract has been validly executed. On the one hand, it has been established in a case from 1976 that the burden of proof ought to be placed on the creditor, as it is the creditor that has an interest in preserving evidence in relation to the execution of the contract, whereas a debtor may find it difficult to prove a "negative action" (i.e. that the debtor has not signed the contract). On the other hand, courts have held that signatures placed on commercial documents in the majority of cases must be deemed authentic, which is why placing the burden of proof on the creditor would be overly burdensome and entail unnecessary transaction costs. In a recent case from an appellate court (2015), it has been further emphasized that where a debtor has a strong interest in the contract, it is the debtor that must prove that it has not signed the contract.

Furthermore, it should be noted that according to a leading legal expert in the field, where a debtor maintains that a document is indeed genuine but that its text has been altered (content-forgery), the debtor retains the burden of proof in substantiating this.

To the best of our knowledge, the courts have yet not examined a civil case where validity of an electronic signature would be contested.

However, some guidance as to how evidence might be evaluated when assessing authenticity of electronic signatures might be found in the preparatory works to the now obsolete Signature Act. The following parameters have been deemed to be of significance in evidence evaluation; (i) the extent to which the systems are verifiable, (ii) the type of information that has been validated by the electronic signature, (iii) the type of legal document concerned, (iv) the circumstance that is to be proved and (v) the relationship of the parties concerned.

Further, additional guidance may be found in the UNCITRAL Model Law on Electronic Commerce, which the Swedish Supreme Court has referred to in several decisions. In article 9 (2) UNICTRAL it is specified how evidence evaluation of electronic signatures is to be performed.

> "Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor."

In light of the above, we are of the opinion that the more advanced electronic signature system is used, the more difficult it will be for a debtor to prove that there has been e.g. a "system failure" resulting in the signature being forged. Further, we believe that if a debtor submitted that the debtor's encryption key has been wrongfully used by an unauthorised person, the burden of proof would be placed on the debtor seeing as the debtor is presumed to have control over own encryption keys. Refuting this presumption will in practice be rather difficult to achieve.

3.4.4 Enforcement

In Sweden, the Enforcement Authority ("KFM") is responsible for the enforcement of both public and private claims. In general, enforcement of a claim is to be based on one of the statutory deeds (i.e. enforcement title (Sw. exekutionstitel)) set out in the Enforcement Code (1981:774), e.g. a court order, an arbitral award, an out-of-court settlement confirmed as enforceable by court (Sw. stadfäst förlikning) or bailiff's order/decision. In simplified terms, this means that enforcement measures may only be taken by KFM when a certain obligation, e.g. for a debtor to make a payment to a creditor, is stipulated in an enforcement title, e.g. a court order.

It should be noted that parties cannot agree that a certain document, e.g. an agreement, is to form the basis for an enforcement action, i.e. that a certain document is to be enforceable.

When applying for enforcement, the original or - if deemed sufficient by KFM - a certified copy of the enforcement title is to be submitted.

However, when an applicant bases its enforcement claim on bearer bonds (Sw. löpande skuldebrev) and other negotiable promissory notes (e.g. bill of lading; Sw. konossement), i.e. documents which upon demonstration entitle the holder of the document (creditor) to payment from the debtor, such a negotiable document must be submitted in the original. This is because a negotiable document, in addition to providing evidence with regard to a certain claim/debt, constitutes a freely transferable current asset. Consequently, once the payment has been made, the payment must be recorded on the e.g. bearer bond and once the debt has been settled the creditor is to return the bearer bond to the debtor.

In light of the above, as far as electronic bearer bonds are concerned, KFM has pronounced (2014) that electronic bearer bonds may not form the basis for an enforcement claim, as it is impossible for KFM to verify and determine (i) whether the submitted electronic document constitutes the original bearer bond and (ii) whether any payment has been recorded on the submitted document. This statement has been contested by Swedish lower courts.

Some lower courts have deemed electronic bearer bonds to constitute merely evidence (certificate) of a claim ("ordinary" promissory notes, Sw. enkelt

skuldebrev), i.e. not a transferable asset entitling to payment upon demonstration, and remanded the cases to KFM for enforcement in line with rules on ordinary promissory notes. Other courts have considered it impossible to determine whether the submitted electronic document is in fact the original one declaring it unenforceable. In a recent judgment (October 2016), one appellate court adjudicated that electronic bearer bonds constitute bearer bonds and that the aforesaid statutory requirement (i.e. that bearer bonds must be submitted in the original) is thus applicable and mandatory.

In a recently issued governmental report (November 2016), it has been emphasized that until clarifying case law has been established by the Supreme Court or new technological solutions introduced (i.e. facilitating verification of the originality of submitted electronic bearer bonds), electronic bearer bonds should not be deemed to constitute a valid ground for an enforcement claim.

In simplified terms, electronic bearer bonds are thus (yet) most likely not enforceable as negotiables ("traditional" paper bearer bonds) under Swedish enforcement law.

With regard to other electronic documents and electronic enforcement titles, these presumably might be submitted (forming the basis for enforcement claim), where KFM finds that a certified copy suffices. Nonetheless, it is unclear whether a certified copy may be presented and submitted electronically. This has recently been discussed in the aforesaid governmental report dated November 2016. In this report it has been proposed that - in order to facilitate electronic filing of enforcement applications - the statutory requirement stating that an enforcement title is to be submitted in the original or certified copy should be repealed in relation to all documents except bearer bonds and other negotiable documents.

3.5 Finland

3.5.1 Applicable law

The use of electronic signatures is accepted in Finnish courts. However, the final value of certain piece of proof is eventually assessed by the Finnish courts in accordance with the Code of Judicial Procedure (4/1734).

The recognition of electronic signatures in legal proceedings in Finland is governed by the Act on Strong Electronic Identification and Trust Services (617/2009, "the Act 617/2009") and the Act on Electronic Services and Communication in the Public Sector (13/2003, "the Act 13/2003"). The latest amendments due to the eIDAS regulation came into effect on 1 July 2016.

The Act on Strong Electronic Identification and Trust Services lays down general principles on strong electronic identification and electronic signatures, as well as on the offering of these services to service providers using them and to the general public.

The Act on Electronic Services and Communication in the Public Sector applies to the lodging of administrative, judicial, prosecution and enforcement matters, to the consideration and to the service of decisions of such matters by electronic means, unless otherwise provided by statute. The Act applies, where appropriate, also to other activities of the authorities. Judicial matters mean matters considered by general courts, administrative courts and special courts.

3.5.2 General principles

The use of electronic signatures is accepted in Finnish courts.

Until 1 of July, Section 5 of the Act on Strong Electronic Identification and Trust Services stated that the legal validity of an electronic signature cannot be denied solely on the grounds that it was concluded electronically. Now this same rule is laid down in Article 25 of the eIDAS regulation. Note that some types of documents may require additional formal requirements under Finnish law, for example, some contract related to real estate. In such cases, electronic signatures may not alone be sufficient.

To prove a valid contract or other document, parties sometimes have to present evidence in court. In such case, electronic signatures may be beneficial with respect to proving the identification of the signatory and creating an assumption that the signatory has in fact signed the document. It could be argued that it is actually easier to prove that an electronic signature is authentic than a handwritten signature, since electronic signature is traceable including a unique link to the signatory. In fact, an electronic signature can prove the existence, authenticity and valid acceptance of a document. Such records are admissible as evidence under Code of Judicial Procedure.

3.5.3 Enforcement

According to Section 9 of the Act on Electronic Services and Communication in the Public Sector, documents delivered in an electronic form to a public authority do not have to be supplemented with handwritten signature. This rule has been confirmed by the legality control for example in decision (3355/6/06, dated 26 June 2008) by the Parliamentary Ombudsman and decision (3666/4/10, dated 20 October 2011) by the Deputy Parliamentary Ombudsman.

Thus, the Act 13/2003 clarifies that in the lodging and consideration of a matter, the required written form is also met by an electronic document delivered to the authorities (Sec. 9). A decision may be signed electronically. The electronic signature of an authority must meet the requirements set out in the eIDAS regulation, i.e. signature shall be an advanced electronic signature or given by using such a method that the originality and integrity of the document can be verified (Sec. 16). At the time of retrieval of decision, the party or the representative of the party shall identify himself/herself by

using for the identification a secure and verifiable identification method (Sec. 18).

It is not stated in the Act 13/2003 that the electronic signature used in relation to the document which is now enforced, is to be a certain type. Thus, primarily, there is no predetermined standard or security level for electronic signature to be used. As a result of latest amendments, the Act 13/2003 now only states that electronic identification method shall be secure and verifiable. In practice, of course, the higher the requirements in relation to electronic signature, the more non-reputable it is as proof.

Note that, in case there is a doubt on the originality or integrity of the document, the authority in question may ask to deliver further proof. A precondition is, thus, that the electronic document contains reliable sender information and there is no reason to suspect the originality or integrity of the document. Finally it is up to a court to assess the final value of certain piece of proof.

Nis Dall