VERSION 1.1

Mike Boyle

DOCUMENT SIGNING AND ESIGNATURES LAWS

GMO GLOBALSIGN LTD

SPRINGFIELD HOUSE, SANDLING ROAD, MAIDSTONE ME14 2LP

TABLE OF CONTENTS

ESIGNATURE FACTS

WHAT IS DOCUMENT SIGNING

Placing a digital signature on a document does not, on its own, make you endorse the contents of a document. Rather, a digital signature is an electronic 'stamp' that (using asymmetric cryptography) serves the double purpose of authenticating sender and/or signee. A third party — called a Certificate Authority (CA) — helps to enable the entire process. Digital signatures are similar to the security certificates you will see on some websites, where a third-party CA vouches for the identity of the certificate-holder. It can be combined with an electronic signature to render the document more secure. In some very sensitive cases, it can be demanded by the document sender to make the signee's consent close to irrefutable.

WHAT ARE ELECTRONIC SIGNATURES

Electronic signatures are categorized as follows:

eSignatures – These typically involve the signer applying their hand-signature mark on the document and then this being protected with a cryptographic digital signature. With basic eSignatures, the crypto digital signature part is created using a single server-held signing key.

Advanced and Qualified eSignatures – Advanced Electronic Signatures (AES) and Qualified Electronic Signatures (QES) – AES and QES provide the highest level of trust and assurance because these use unique signing keys for every signer. This directly links the user's identity to the signed document such that anyone can verify it on their own using an industry standard PDF reader. Furthermore, as the signer has sole control of their unique private signing key this ensures non-repudiation, i.e. even the service provider cannot be held responsible for creating the signature. The advantage of using AES/QES is that they show exactly who signed the document.

WHAT IS A DIGITAL CERTIFICATE

A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate.

Just like a passport, a digital certificate provides identifying information, is forgery resistant and can be verified because it was issued by an official, trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.

To provide evidence that a certificate is genuine and valid, it is digitally signed by a root certificate belonging to a trusted CA. Operating systems and browsers maintain lists of trusted CA root certificates so they can easily verify certificates that the CAs have issued and signed. When PKI is deployed internally, digital certificates can be self-signed.

WHICH COUNTRIES LEGALLY RECOGNIZE DIGITAL CERTIFICATE CREATED ESIGNATURES?

Each country recognizes the legal basis of both certificate based digital signatures and standard electronic signatures, differently and in their own way. Adobe has made available a comprehensive summary of the applicable laws in each country, which define whether or not a digitally signed PDF document will be permissible in law.

Here is the summary for each country, as described by Adobe:

https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-electronic-signatures.pdf

WHO IS GLOBALSIGN AND WHAT IS THEIR ROLE

GMO GlobalSign is a public Certificate Authority (CA) and an Adobe Approved Trust List (AATL) member, providing cloud-based PKI solutions. Our identity platform allows enterprises to deploy secure e-services, manage employees and Enterprise identities, and automate PKI deployments for the hyper-connected world of mobile devices, users and machines.

Certification Authorities, such as GlobalSign (who verify the identities of businesses and individuals and issue digital certificates base upon them) do not have any control over the legal acceptance of a digital certificate based electronic signature. These are specific to the laws of each country as to how they have chosen to legally interpret them. That said, GlobalSign's role as an AATL member requires us to create and control cryptographic key material in a manner compliant to the AATL Technical Regulations (see WHAT ARE THE AATL TECHNICAL REQUIREMENTS?)

WHO IS ADOBE® AND WHAT IS THEIR ROLE

The Adobe Approved Trust List (AATL) consists of member organizations from around the world and includes the members of the European Union Trust List (EUTL). They provide certificates that enable creation of trusted digital signatures, whenever the signed document is opened in Adobe Reader® or Acrobat®.

GlobalSign is a recognized, compliant AATL member:

https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html

WHAT IS AATL

The Adobe Approved Trust List (AATL) is a program that allows millions of users around the world to create digital signatures that are trusted whenever the signed document is opened in Adobe Acrobat or Reader Software. Essentially, both Acrobat and Reader have been programmed to reach out to a web page to periodically download a list of trusted "root" digital certificates. Any digital signature created with a credential that can trace a relationship ("chain") back to the high-assurance, trustworthy certificates on this list is trusted by Acrobat and Reader.

WHAT ARE THE AATL TECHNICAL REQUIREMENTS?

Adobe has a specific set of Technical Requirements that define and impose specific rules that both the CA and the controller of the supplied end entity certificate must follow.

The Technical Requirements are set out on Adobe's website, here:

https://helpx.adobe.com/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/file.res/aatl_technical_requirements_v14.pdf

These Requirements make the following references:

Non-governmental members must have successfully passed within the past 18 months, and continue to pass on an annual basis, any or all of the following:

4.1. WebTrust for CA audit;

4.2. ETSI 101 456 audit;

4.3. ETSI 102 042 audit;

4.4. ISO 21188:2006; and/or

4.5. German Digital Signature Law audit

AATL TECHNICAL REQUIREMENTS - SERVICE PROVIDER/USER

4.1. WebTrust for CA audit;

4.2. ETSI 101 456 audit;

4.3. ETSI 102 042 audit;

4.4. ISO 21188:2006; and/or

4.5. German Digital Signature Law Audit

AATL TECHNICAL REQUIREMENTS - THE CA

4.1. WebTrust for CA audit

GLOBALSIGN'S AATL TECHNICAL REQUIREMENTS CONFORMITY CERTIFICATE/STATEMENT

GlobalSign is regularly audited to the CA industry regulations, WebTrust. Our WebTrust audit covers our compliance in line with the AATL Technical Requirements.

Our WebTrust compliance reports can always be found on our www.globalsign.com website through each of the WebTrust Seals.

Here is the link to the current WebTrust report:

WebTrust Seal: https://cert.webtrust.org/SealFile?seal=2056&file=pdf