Implementation of Qualified Electronic Signatures

Author: Dr. Andreas Schwinn, Roche Pharma*)
Correspondence: Dr. Andreas Schwinn | Roche Pharma AG, Emil-Barell-Str. 1, 79639 Grenzach-Wyhlen | andreas.schwinn@roche.com

Abstract

The pharmaceutical industry has developed their electronic signature concepts based on CFR part 11 requirements. Applicable EU (or also Swiss) requirements on electronic signature standards are not widely adapted, in particular the standards: Qualified Electronic Signature (QES) and Advanced Electronic Signature (AdES). This publication sheds some light on the legal and technical backgrounds and appeals to use compliant signature standards throughout the Pharmaceutical Industry in Europe. The author describes the successful implementation of Qualified Electronic Signatures at Roche Pharma AG, Grenzach.

Keywords

Electronic signature | Paperless Office | Qualified Electronic Signature (QES) | eIDAS regulation | Non-compliance

Introduction

Back in the Middle Ages, when most people could not read or write, documents were often signed with an "X" or with "XXX". The connotation is that the "X" represents the Christian Cross, and "XXX" visualizes the crucifixion scene. This way, people meant the document to be literally signed in God's name. The author found this scenery touching on many levels and decided to use it in this publication.

Today the "X"/"XXX" signature is seen as a symbol of illiteracy. Analphabetism is still a serious problem in developed countries: In Germany, there are 2.5 million analphabets and 7.5 million functional analphabets [2,3] on about 80 million inhabitants.

Thus, it is not analphabetism that is being discussed here – it is rather a new form of digital illiteracy. Today, the topic is signing documents electronically.

The electronic signature standard in the EU and Switzerland is called Qualified Electronic Signature (QES). QES is considered legally equivalent to a handwritten signature.

One might ask:

Why is a QP interested in QES?

A qualified person is used to provide declarations with legal implications, for the content of which they can be held legally liable (QP declarations, confirmations, statements, etc.). In a GMP world, it is assumed that such declarations must be signed. In times of digital transformation, this signature should be electronic.

For signing documents electronically, Directive 1999/93/EC, implemented the concept of the Qualified Electronic Signature (QES) in EU Legislation. The directive was replaced by the eIDAS regulation (EU) 910/2014 [4], the concept of the QES remains.

In Switzerland, this concept is covered by ZertES [5]. When looking at electronic signature concepts in the pharmaceutical industry, one will learn that although existing for 25 years, the concept of QES is not widely adapted.

Electronic Signatures

It is impossible to write this publication without bone-dry technical and legal details. For the reader who is more interested in the message than the details, the sections that are difficult to read have been marked:

Passages that are very technical or legal in nature, where the author made the experience that people stopped listening to him when he tried to explain them, are marked with italic fonts. Whenever you see this, please feel free to skip.

*) Author's Note: Statements presented herein reflect the interpretation and opinion of the author, not an official Roche opinion, nor an opinion of the German Qualified Person Association (GQPA). To learn more about electronic signatures, the author recommends starting with the e-signature Knowledge Base – European Commission [1].

Pharm. Ind. 86, Nr. 7, 652–656 (2024)

Certificate-Based Signatures

There are electronic signatures that are certificate-based, and others that are not. Certificate-based signatures are also called digital signatures.
Note: Not every electronic signature is a digital signature.

As the name says, such signature is based on a digital certificate. This digital certificate can be thought of as one's digital fingerprint.

The technical explanation: A digital certificate is a set of information that is stored securely on user's device (e.g. the Windows Certificate Store or in the Apple Keychain). The certificate contains e.g. the user name, the issuer, a public and a private key. The private key is used for the digital signature. The signature process means encryption of document information. The public key is used to validate the signature. If the validation is successful, it means that the signatory is authenticated as the certificate owner and the document was not changed after the signature.

Certificate-based signing is not only used to sign documents: It is the basis for email encryption, secure webpages, secure login, code signing, and more. Obviously, certificate-based signing is the basis for digital transformation.

This article will tell the readers that certificate-based signing is the only correct way to sign documents (for readers in the EU or Switzerland).

Non-certificate-based Signatures

Non-certificate-based signatures are typically Simple Electronic Signatures (SES) as defined below.

Signature Types in the European Legislation

The eIDAS regulation knows 3 types of electronic signatures:

- Simple Electronic Signature (SES)
- Advanced Electronic Signature (AdES)
- Qualified Electronic Signature (QES)

Simple Electronic Signature (SES)
SES is mentioned in the eIDAS regulation as "trust services that are used exclusively within closed systems". This is the standard for e.g. an enterprise resource planning (ERP), electronic document management system (EDMS), or laboratory information management system (LIMS). No further requirements are specified for SES in eIDAS.

In the pharmaceutical industry, such signatures are expected to comply with CFR part 11 [6].

Note: In an EDMS, the document is not signed, but an SES is recorded in the signature audit trail. The system will link the SES to the document. With certificate-based signatures, the signature with all its digital properties is a part of the document.
It is important to consider, that such an SES can only be fully authenticated within this so called "closed system". A document downloaded from an EDMS as a PDF document can be edited by an average 12-year-old. In the case of a printout, there is no way to prove the authenticity of the document without access to the EDMS.

Conclusion: SES is for Closed Systems.

Advanced Electronic Signature (AdES)
An advanced signature is a certificate-based signature (see above).

The technical/regulatory definition from eIDAS:
"Article 26
Requirements for advanced electronic signatures:
An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable."
This passage needs translation:
First hint: "electronic signature creation data" from §26(c) means the digital certificate. The certificate identifies the signatory (§26(b)) since it contains the

Dr. Andreas Schwinn
is a Pharmacist and Qualified Person. He started his industry career at a Contract Research Organisation (CRO)/Contract Manufacturing Organisation (CMO) establishing the units Clinical Trial Supply business as a respected service provider in the field. During this time, he acquired the qualified person (QP) qualification in 2005. In 2013, he joined Roche Pharma AG as QP for investigational medicinal product (IMPs). After heading the Release Preparation Team for several years, he is now Senior QP for IMPs.

signatories name in the "subject field". It is uniquely linked to the signatory (§26(a)), if he has control over the certificate (user-specific installation in the certificate store). §26(d) describes a standard property of certificate-based signatures that modifications are easily detectable (e.g. annotations) or completely prohibited (any kind of editing of the text or the document structure).
The eIDAS compliant standards for Advanced Electronic Signatures are described in Commission Implementing Decision (EU) 2015/1506 [7], and they are all certificate-based. Other standards would be technically possible, thus, there is none approved.

Currently, there are no other accepted ways to achieve Advanced Signatures than with digital certificates (A public key infrastructure – PKI).

Qualified Electronic Signature (QES)
A Qualified Signature is an Advanced Signature where the certificate is issued by a qualified trust service provider and is stored in an extra-secured place, e.g. a USB token or a secured server.

eIDAS says: "'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures".
Qualified certificates are issued by qualified trust service providers, institutions that are under the supervision of notified bodies, officially authorized, and published in the EU/EEA Trusted List Browser [8].
Qualified electronic signature creation device means a safe place to store the private key of a certificate. This can be e.g. a USB token, smart card, a server in the cloud, or a hardware storage module (HSM) in the network.

CFR 11 Requirements

In 1997, the FDA has published fundamental requirements on electronic signatures. These requirements include e.g.

- printed name of the signer;
- date and time;
- the meaning associated with the signature;
- signatures shall employ at least 2 distinct identification components (e.g. user ID and password);
- and more

CFR 11 was the basis for the pharmaceutical industry to develop their signature concepts.
Note: QES is typically CFR part 11 compliant.[1)]

[1)] QES is CFR 11 compliant in the great majority of set-ups. Otherwise with configurational or procedural controls.

Signature Concepts in the Pharmaceutical Industry

The most prominent signature solutions in the pharmaceutical industry are:

1. For closed systems (ERP, EDMS, LIMS etc.): Simple Electronic Signatures (SES), typically fulfilling the requirements of CFR part 11.
2. For documents (that are e-signed outside of an EDMS): Certain e-signature tools are used (e.g. DocuSign® and Adobe Sign®, to name the most prominent ones). Such tools provide very useful workflow mechanisms, and authentication via email and phone.
3. Such e-signature tools can provide QES, thus, they are often not configured to do so.
4. Per default, the signature mechanism in such e-signature tools does not comply with the AdES or QES definition provided by eIDAS regulation.

There is no certificate used to authenticate the signatory.
The authentication mechanism is based on unique IDs assigned to each signing process (envelope). With these IDs, signature summaries (aka Certificate of Completion) can be retrieved from the cloud application to verify the authenticity of the signed document.
These signature summaries have no legal meaning in the EU, apart from representing an SES-signed document in a closed system.
The fact that those signature solutions are CFR part 11 compliant or formally validated does not change the assessment. If validation means to provide evidence that an application is suitable for its intended purpose, and the signature solution does not provide a real signature, the question should really be asked whether the system has been validated.
The name of this signature summary "Certificate of Completion" has misled quite a few users to believe that they have a certificate-based signature (which is an obvious misconception: see above for the definition of digital certificate).
To complicate things, the e-signature tool will use certificate-based signing to secure the document against changes. The signature information identifies the e-signature tool vendor in California as the signatory. In an EU framework, the document was not signed by the user, but by the e-signature tool vendor. Since a company in California is neither a "qualified trust service provider", nor an EU authorized notary, this does not seem right.

In summary, documents processed with such e-signature tools are "pseudo-signed". Such "pseudo-signature" has no legal relevance as a signature in the EU.

Pharm. Ind. 86, Nr. 7, 652–656 (2024)

What e-Signature tools should be used for

Note: contracts do not need to be signed. This makes the mentioned e-signature tools an ideal solution for contracts or quality agreements. They provide useful workflow mechanisms that makes contract management easy.

It should therefore not be claimed that contracts are signed. The author strongly recommends avoiding phrases like "this contract becomes valid if duly signed by all parties" or "this contract requires the written form". Both statements require the contract to be signed with a valid signature. If they are "pseudo-signed" with the mentioned e-signature tools, masses of contracts that are invalid by default will be produced.

In summary: Contracts are typically pseudo-signed; thus, it is ok.

Pharmaceutical companies are non-compliant

In conclusion, there is an EU standard for electronic signatures, but most pharmaceutical companies do not apply it. Instead, they apply "pseudo-signatures" without a legal meaning. Obviously, the standard is not really enforced by authorities.

It is known that single GMP inspectorates in Germany require QES as signature standard for electronic documents. Deficiency letters have been observed from EU Health Authorities for submitting documents that require a signature (e.g. the Clinical Protocol) signed with non-compliant signature standards.

How can pharmaceutical companies become compliant?

This was the question that the QP organisation at Roche Pharma AG, Grenzach, raised in late 2019. The need to implement a compliant way to sign QP declarations, QP confirmations, and other QP statements was recognized – back then these were signed on paper.

Introduction of QES at Roche Pharma AG Grenzach (RPAG)

The objectives of this project were, to

- establish QES
- assure that all signed documents that are shared with 3rd parties are signed with QES
- make qualified certificates available to all users that need it
- fulfill QES standards as per eIDAS (EU) and ZertES (CH)
- enable QES with DocuSign – Roche's corporate e-signature tool; this means implementing a DocuSign instance that is QES and CFR part 11 compliant; and advertising its use
- implement QES with PDF Editors – a signature option for documents not requiring a signature workflow
- implement a PDF-based, paperless documentation concept that fulfils GMP and Data Integrity requirements
- change all paper-based processes in the QP certification group to paperless
- validate the system as per corporate standards
- integrate the concept into the corporate IT infrastructure

It took a while to learn the basics of digital signing, and to understand the requirements of the eIDAS regulation in full. Another struggle was to identify suitable qualified certificates and the respective trust service providers. Several certificates need to be tested before the certificate(s) best suited to the user's needs are found. Then the paperless business processes need to be defined. This requires new paperless GMP rules. Validation needs to be done. RPAG also integrated the solution into the corporate IT landscape with regard to validation, entitlement management, training, IT support, lifecycle management etc.

RPAG implemented QES for use with PDF-editors as well as with DocuSign®.

Thus, RPAG decided to use DocuSign only when signature workflows are required, and in particular for contracts/quality agreements.

All previously paper-based processes have been replaced by PDF-based, paperless processes with QES.

The last document replaced was the certification register for manual releases (for the certifications that occur outside of Roche's ERP systems). It is worth noting that this concept has even been applied to the certification register – evidence of considerable confidence that the process has no weak spots with regard to GMP compliance, data integrity, and validation.

The journey lasted 3 years from first start to full completion. The foundation was laid in the first 2 months of the COVID-19 epidemic under an emergency change.

Costs of QES

QES is associated with the conception that it is very cumbersome and expensive:

In fact, a signature can be 2 clicks and a password, applied in less than 5 sec. The upfront investment was half an FTE-year of work. With the knowledge available today, it could be repeated in half the time.

The costs per signature depend on the selected trust service provider. The option, which was implemented at Roche Pharma AG, Grenzach, creates costs of 0.03–to 0.26 euros per signature (pricing model per employee/per certificate – not per signature/estimating 200–1,500 signatures/year).

For the Option that shall provide ZertES compliance for Roche's Swiss colleagues, the costs are starting with 1.15

Swiss francs (pricing model: per signature – it should become cheaper with a greater user base).

Benefits of QES and paperless office

The benefit calculation is always based on assumptions: For example, Roche has all relevant paper documents stored electronically in an EDMS anyway (accordingly, the calculation does not include the costs for an EDMS since those did not change).

The Roche Quality Group in Grenzach works together with many external partners: Accordingly, there were quite a few paper-based processes that were not implemented in the corporate IT systems.

The obvious benefits are:

- no printing
- no paper, printer and printer consumables
- no wet signature logistics
- no scanning
- no paper filing
- no folders
- no shelves
- no paper-based archiving
- no external archives for long-term storage

Direct costs have been significantly reduced from the start – and when all benefits will be fully realized, it is expected to save around 5,000 euros/employee/year.

The biggest benefit comes from the increased productivity which was estimated at 10 %.

Another cost factor was the Roche group in Grenzach decided not to use DocuSign (Roche's corporate e-signature tool) for internal documents, but to sign with PDF editors (at no extra costs). The pricing model for DocuSign would have been per envelope and per signature. The respective savings are a lower single digit euro value per each signature + envelope.

Conclusion

Readers who have read this far, will not be surprised that the conclusion is positive.

- QES was introduced with a reasonable investment.
- Significant savings and efficiency gains were achieved.
- Roche has closed a compliance gap – its electronic signatures are legally valid.
- All GMP processes are paperless.
- Meanwhile, several hundred colleagues in the EU organisations are using QES.

Moreover, the Roche Quality Group in Grenzach acquired digital competence and is now signing with a real signature, no longer with the digital equivalent to "XXX".

References

[1] eSignature Knowledge Base – European Commission; *https://ec.europa.eu/digital-building-blocks/wikis/display/ESIGKB/What+are+the+levels%2C+simple%2C+advanced+and+qualified+of+electronic+signatures*

[2] Funktionaler Analphabetismus in Deutschland – Größenordnung, Ursachen, Interventionen May 2019, Zeitschrift für Neuropsychologie. 30 (2):87–95; *https://www.researchgate.net/publication/333470247_Funktionaler_Analphabetismus_in_Deutschland_-_Grossenordnung_Ursachen_Interventionen*

[3] Wenn Menschen mit drei Kreuzen unterschreiben, Welt, 11.09.2011, Claudia Guderian; *https://www.welt.de/wissenschaft/article13595183/Wenn-Menschen-mit-drei-Kreuzen-unterschreiben.html*

[4] 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. Official Journal of the European Union 28.8.2014; *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910*

[5] Fedlex. 943.032 Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES) vom 23. November 2016 (Stand am 2. Oktober 2020); *https://www.fedlex.admin.ch/eli/cc/2016/753/de*

[6] U.S. Food and Drug Administration. CFR Part 11, Code of Federal Regulations Title 21; *https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1&subpartNode=21:1.0.1.1.8.1*

[7] Commission Implementing Decision (EU) 2015/1506, of 8 September 2015, laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Official Journal of the European Union. 9.9.2015; *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1506*

[8] European Commission eIDAS Dashboard. EU/EEA Trusted List Browser; *https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home*

The links were last accessed on 23 Apr 2024.

Redaktionsleitung (V. i. S. d. P.): Andreas Gerth. Redaktionsassistentin: Vanessa Dobler. Verlag: ECV · Editio Cantor Verlag GmbH, Baendelstockweg 20, 88326 Aulendorf (Germany). Tel.: +49 (0) 7525-940 0. E-Mail: redaktion@ecv.de. www.ecv.de. Herstellung: rdz GmbH.