Thomas Zefferer, Arne Tauber, Bernd Zwattendorfer, Thomas Knall: "Secure and Reliable Online-Verification of Electronic Signatures in the Digital Age". In Proceedings of the IADIS International Conference WWW/INTERNET 2011, pp. 269-276, IADIS, 2011.

SECURE AND RELIABLE ONLINE-VERIFICATION OF ELECTRONIC SIGNATURES IN THE DIGITAL AGE

Thomas Zefferer, Bernd Zwattendorfer, Arne Tauber, Thomas Knall
A-SIT Secure Information Technology Center – Austria – IAIK, Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

ABSTRACT

With the rise of the digital age, electronic signatures have become an important tool to express written consent especially in security sensitive fields of operation such as e-Government or e-Business. Being legally equivalent to handwritten signatures in many countries, electronic signatures guarantee integrity and non-repudiation of origin. Reliable verification of electronic signatures is a crucial element in various electronic signature based solutions. A myriad of document and signature formats, complex cryptographic algorithms, and various additional requirements complicate the verification of electronic signatures. Amongst others, security, usability, and privacy preservation can be identified as key requirements for the reliable verification of electronic signatures.

In this paper we introduce a central web application based signature verification tool. We discuss general requirements of such tools and show how the identified requirements are met by the presented solution. The presented tool plays a central role in the Austrian e-Government infrastructure and has been in productive operation for more than four years. Although being originally developed for the Austrian e-Government, the tool is also applicable in an international context. Due to its modular and scalable design, the presented verification tool is well prepared to overcome the challenges of a globalized digital future.

KEYWORDS

Electronic signatures, verification, web application, document format detection

1. INTRODUCTION

Signatures have been the most important means to prove authenticity and to provide written consent since the Early Middle Ages. Still, handwritten signatures play an important role in our daily life and are frequently used in various scenarios such as the signing of legally binding contracts or authorization of financial transactions.

During the past few decades, information and communication technologies (ICT) have significantly changed our daily life. An increasing number of services are provided over the Internet nowadays. Amongst others, this includes services from security and privacy sensitive fields such as e-Banking or e-Government. Governmental, administrative, and financial procedures often require the provision of users' written consent. In the physical world, written consent is usually provided by means of handwritten signatures. The mapping of traditional procedures to the digital world therefore raises the demand for a digital equivalent to handwritten signatures.

This demand is met by electronic signatures. Electronic signatures rely on public key infrastructures (PKI) (Housley, 2002) and asymmetric cryptographic algorithms such as RSA or ECDSA. Basically, electronic signatures guarantee integrity and non-repudiation of origin. In various countries, the legal impacts and equivalence of electronic signatures to their handwritten pendants are ensured by national laws. There are few references providing a common understanding and rules for the application of electronic signatures. One of these references is the European Union (EU) Signature Directive (European Union, 1999). EU Member States are obligated to ratify this directive, which has been enacted by the European Parliament and the Council in the year 2000. This means that Member States have to transpose the directive into national law in order to assure legal equivalence between handwritten signatures and qualified electronic signatures on European level.

The technical verifiability of electronic signatures is one of the most relevant advantages compared to handwritten signatures. Given an electronically signed document and the publicly available signing certificate, the correctness and validity of the electronic signature can be determined unambiguously by applying appropriate cryptographic verification methods. This way, non-repudiation of origin is guaranteed, i.e. the signer cannot deny having signed a certain document. Therefore, each modification of the signed document automatically invalidates the applied signature. This way, the application of electronic signatures ensures the integrity of the signed content.

Reliable identification of the signatory and verification of signed contents' integrity raise the demand for appropriate verification mechanisms. Unfortunately, a plethora of cryptographic signature algorithms and standards, different document formats, and complex PKI infrastructures render the implementation and operation of reliable and usable verification tools difficult. Today we can find a heterogeneous ecosystem of electronic signature formats based on different policies throughout Europe and the whole world. The ongoing trend towards a single digital market raises the demand for a common understanding of different signature formats. In the EU, the European Commission has tried to limit the development and use of different signature formats. Although the EU Signature Directive provides a first basis for regulating the application of signatures, detailed formats for cross-border use have not been specified. This is regulated by the Commission Decision 2011/130/EU (European Union, 2011) of February 2011, which specifies in detail the cross-border use of XML[1], CMS[2], and PDF[3] advanced electronic signatures being conformant to the EU Signature Directive. Nevertheless, even if first regulations came up, the current electronic signature ecosystem is not limited to those three types, but comprises far more formats.

In this paper, we discuss requirements of electronic signature verification tools and introduce the approach we have followed to provide users with a reliable and usable tool for verification of electronic signatures of different formats. The remainder of this paper is structured as follows. We first define basic requirements for signature verification tools in Section 2. In Section 3 we introduce our web application based solution and show that it satisfies the predefined requirements. Finally, conclusions are drawn in Section 4.

2. DEFINITION OF REQUIREMENTS

For all electronic signature based solutions, provision of reliable signature verification mechanisms is mandatory. Only if recipients of electronically signed documents are able to reliably verify the obtained electronic signature, integrity and authenticity of signed documents can be assured. The development of appropriate signature verification tools is actually a complex task that requires the consideration of various aspects and requirements. In general, reliability and security, usability, scalability, availability, and privacy preservation can be identified as core requirements for signature verification tools. In this section we discuss the relevance of these key requirements in more detail.

Reliability and Security

Reliability is crucial for any signature verification tool. Reliability implies that the used verification tool exactly shows the expected behavior at any time. This basically means that the tool reliably distinguishes between valid and invalid signatures. Incorrect verification results are not acceptable, as users must be able to trust the provided results. Since qualified electronic signatures are legally equivalent to handwritten signatures, incorrect verification results can have serious consequences. For instance, the wrongly successful verification of forged contracts can pave the way for fraud and potentially lead to serious financial losses.

To achieve reliability, appropriate quality assurance techniques have to be applied during the development of signature verification services. For instance, this implies the reliance on approved design patterns and development tools as well as the utilization of comprehensive testing frameworks.

---

[1] Extensible Markup Language (XML) advanced electronic signatures, see ETSI (2006)
[2] Cryptographic Message Syntax, see Pinkas et al. (2008)
[3] Portable Document Format (PDF) advanced electronic signatures, see ETSI (2009)

Besides reliability, security is another key requirement for signature verification tools. Because of their relevance, such tools pose a potential target for various attacks. Attackers may be interested in forging signature verification results to trick users into accepting invalid signatures and forged signed documents. As a compromised verification tool can obviously threaten the reliability of signature verification processes, appropriate protection mechanisms are crucial for any signature verification tool.

Usability

Besides functionality, usability is another key requirement. Recent developments in the IT sector have shown that usability often displaces functionality as most relevant acceptance criterion. For electronic signature based software solutions, usability is a crucial issue due to the complexity of electronic signature schemes.

The creation and verification of electronic signatures usually comprises the application of different cryptographic algorithms, the communication with hardware tokens such as smart cards, and the interaction with various remote components of the underlying public key infrastructure. However, the majority of users are neither interested in technical details nor capable of understanding complex cryptographic concepts but prefer intuitive and clear processes. To comply with the demand for usability, the suggestions described below should be taken into account during design and development of verification tools for electronic signatures.

Platform Independence

Platform independence is mandatory in order to make software solutions accessible to a broad spectrum of users. Especially for e-Government services, platform independence is a crucial requirement as these services must be usable by all citizens and discrimination of certain user groups is not acceptable. In case of web based solutions, the demand for platform independence has to be complemented by the requirement for web browser independence.

Considering the fact that electronic signatures are frequently used within e-Government solutions, platform (and web browser) independence can be identified as a fundamental requirement for signature verification tools.

Avoidance of Local Software Installations

Experience has shown that the need for local installations can significantly reduce the usability of software solutions. Inexperienced users may back off from carrying out software installation procedures on their local system. Especially for e-Government solutions, which have to be accessible to all users irrespective of their familiarity with computers, installation-free approaches are thus preferable. Moreover, certain company networks' policies disallow installation of foreign software products on local network machines. Hence, server based approaches are the favored choice.

Given a frequent usage of electronic signatures in the e-Government domain, the avoidance of local software installations can be identified as another usability improving requirement.

Hiding of Complexity

Correct verification of electronic signatures is basically a complex task. Depending on the underlying signature standard, several data transformations and cryptographic operations have to be carried out in order to determine the validity of a given signature. Additionally, various central data sources have to be accessed in order to verify the validity of the used signing certificate.

From the users' point of view, this complexity is of little interest. Users only want to know whether an electronic signature is actually valid or not. The provision of too much information during the verification process might confuse users and complicate the use of the verification tool. To improve usability, signature verification tools should therefore hide as much complexity from users as possible and focus on correct determination and clear presentation of results.

Single Point of Contact

With the increasing popularity of electronic signatures, users are faced with a growing number of document and signature formats. In the e-Government sector, the situation is even intensified by ongoing interoperability attempts between different countries. Since users are more and more able to access e-

Government services from other countries, users are increasingly faced with foreign country specific electronic signature formats.

Due to given differences in document and signature formats, usually each format requires a specific verification service. Hence, the emerging number of document and signature formats leads to a vast number of associated verification tools. From a usability point of view, this is far from being ideal and complicates the generic verification of electronic signatures significantly.

For a usable signature verification tool we can thus define a single point of contact for all documents and signature formats as key requirement. A one-for-all approach renders the maintenance of different verification tools unnecessary and significantly improves usability.

Simplicity

To improve the acceptance of electronic signature based services, simple and intuitive solutions are mandatory. Users are not interested in spending their time in studying manuals and documentation. Thus, interaction with signature verification tools should be as simple and straightforward as possible. Ideally, users should only be required to provide the respective signed document for verification. The provision of additional verification parameters could lead to dubiety and should be omitted whenever possible.

Scalability

Scalability can be identified as another key requirement for signature verification tools. Regarding the increasing popularity of electronic signatures and the ongoing attempts to make national signature based solutions also accessible across national borders, a growing number of document and signature formats can be expected. A one-for-all solution that covers all document and signature types therefore has to allow an easy integration of new document and signature formats. A scalable and modular design can thus be identified as another key requirement for signature verification tools.

Availability

In certain scenarios, the immediate verification of electronically signed documents can be crucial. In such situations, the unavailability of appropriate verification means might lead to financial losses or other negative impacts. Availability thus defines another important key requirement.

Privacy Preservation

In many cases, electronically signed documents contain confidential or privacy sensitive data. Document owners therefore usually have a high interest in keeping these data undisclosed. Especially server based verification tools seem problematic in this context as they require potentially confidential documents to be uploaded to a central server. The application of appropriate privacy preserving protection mechanisms is therefore a key requirement especially for server based verification solutions.

3. ARCHITECTURAL DESIGN AND IMPLEMENTATION

Reliability and security, usability, scalability, availability, and privacy preservation have been identified as key requirements of successful verification tools for electronic signatures. In this section we introduce a signature verification tool that basically fulfills all identified requirements. The presented tool has already proven its suitability for daily use during more than four years of productive operation[4]. Our solution follows a web application based approach. This way, it improves usability by avoiding the need for local software installations. Also, a web application based approach satisfies the previously identified requirement for platform independence. Figure 1 shows the tool's web based user interface.

[4] The tool is currently hosted by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) and is publicly available at https://www.signaturpruefung.gv.at.

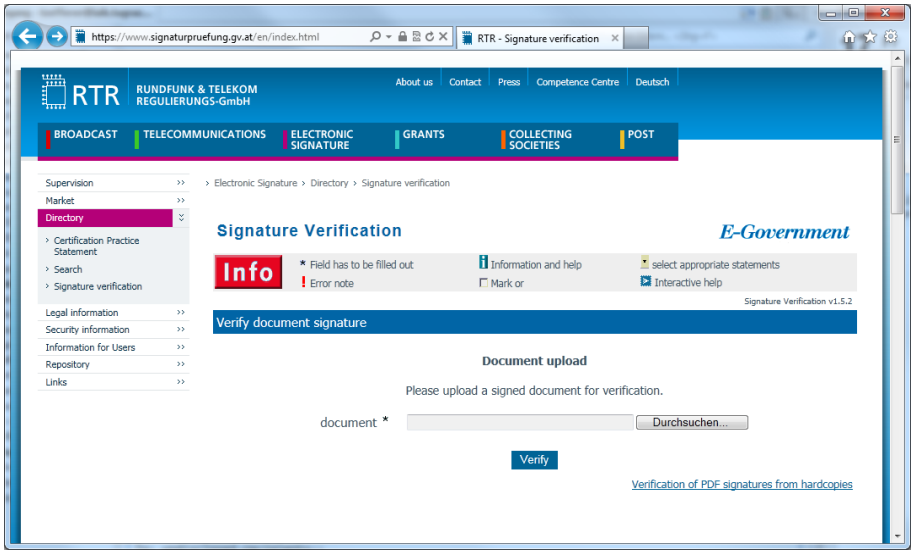

Figure 1. Web based user interface of the presented signature verification tool. Users can verify electronically signed documents by uploading them to a central service.

By omitting unnecessary input and output elements, the implemented user interface also satisfies the requirement for simplicity. Users can start the verification process by selecting and uploading the document to be verified and by subsequently pressing the 'Verify' button. Users do not have to take care about the applied signature algorithm and do not need to enter additional information about the document format. Thus, from the users' point of view, the entire verification process is kept as simple as possible. After completion of the verification process, the obtained results are presented in the users' browsers as illustrated in Figure 2.

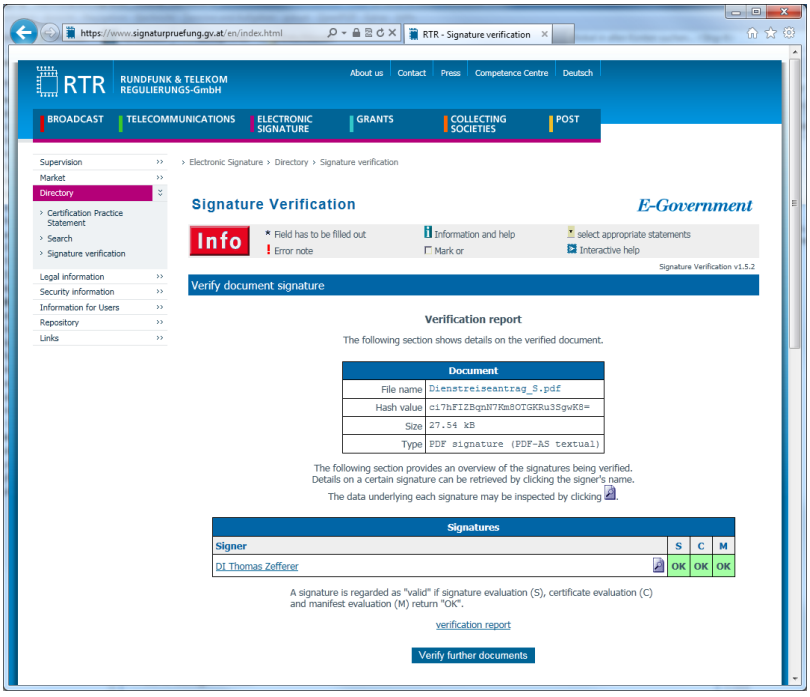

Figure 2. Presentation of the signature verification results.

Again, the design of the user interface has been kept minimalistic. Most details of the verification process are hidden from the user. The results of the verification process are summarized in two basic tables. This

way, the verification result is apparent immediately and users are not bothered with additional and probably confusing technical details[5].

Although its minimalistic user interface makes the proposed signature verification tool appear rather simple at a first glance, the business logic behind the user interface is actually quite complex. Figure 3 shows the basic internal architecture of the tool.

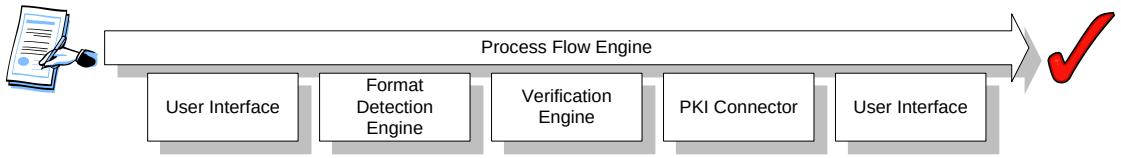

Figure 3. Basic architecture of the signature verification tool.

The *Process Flow Engine* controls the entire sequential verification process. The document to be verified is retrieved via a web based *User Interface* component. The format of the retrieved document is subsequently determined by the *Format Detection Engine*. After successful determination of the format, the *Verification Engine* verifies the document's electronic signatures. The *PKI Connector* component is used to connect the verification tool to external public key infrastructures in order to verify the validity of signing certificates and to retrieve related identity information of signatories. The result of the verification process is finally presented via the web based *User Interface* component.

The *Format Detection Engine* assures that the presented verification tool supports processing of files and documents irrespective of their format. This satisfies the requirement for provision of a single point of contact, as one and the same user interface can be used to upload and verify multiple types and formats of documents and electronic signatures.

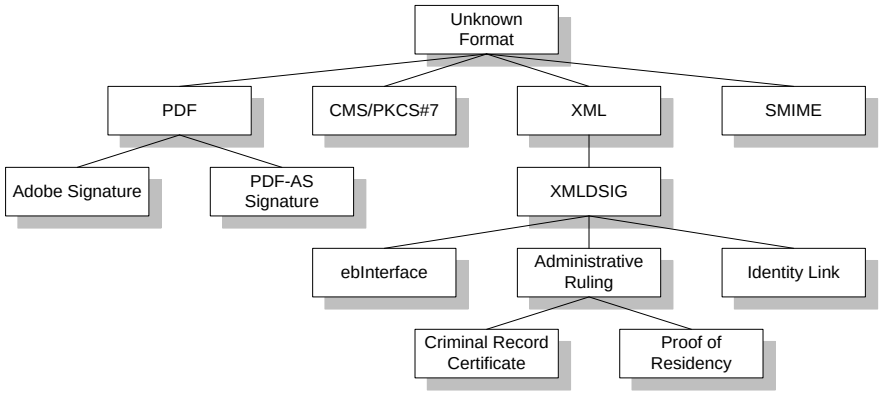

Figure 4. Modular format detection approach. Each node of the tree represents a certain document format.

To achieve scalability, the *Format Detection Engine* follows a modular and extensible approach. Basically, the document-format hierarchy shown in Figure 4 is implemented. Each node in the hierarchy tree represents a certain document class that implements a recognition mechanism for the particular format. Each format-detection process starts at the root node. If a node 'accepts' a given document, the node's child nodes are recursively investigated until the document format has been determined unambiguously. The hierarchy is defined by an internal XML based configuration and covers all document formats supported by the verification tool[6]. Another XML file is used to assign so called verifiers to each detected document and signature format. Verifiers are part of the *Verification Engine* and basically implement required cryptographic operations to appropriately verify electronic signatures of a certain format. Due to the followed

[5] A detailed (signed) report about the applied verification process can still be downloaded by following the displayed link ‚verification report'. Additional information about the signer of the document can be accessed by clicking the signer's name in the lower table.

[6] Note that the hierarchy illustrated in Figure 4 is just an incomplete example and does not cover all supported document formats.

hierarchical approach, the document-detection and verification process can be carried out efficiently. Additionally, new document formats, format detectors, and verifiers can be added to the existing solution easily without harming the tool's performance significantly. This satisfies the previously identified requirement of scalability and contributes to the sustainability of our solution.

Besides increasing usability, a central approach also improves security. Client-side solutions are in general more prone to attacks as they need to be installed and run on client systems that often lack appropriate protection mechanisms against malware. Our solution avoids this issue by encapsulating all functionality in a central server component, which can be professionally protected by a safe and secure operational environment[7].

Unfortunately, a central approach bears several challenges too. Regarding the previously defined requirement for availability, a central approach might be disadvantageous as users require a working Internet connection to gain access to the provided service[8]. However, as nowadays nearly all desktop PCs, laptops, and even smartphones are connected to the Internet, this requirement should be easily grantable.

Fulfillment of the requirement of privacy preservation turns out to be far more challenging for server based verification tools than for local installations. As potentially confidential and privacy sensitive documents need to be uploaded to a central server, appropriate protection mechanisms need to be implemented by the verification tool. Our solution assures the preservation of privacy and confidentiality on transport level by securing data transmissions between the user and the tool using the HTTPS and transport layer security (TLS) protocols. Furthermore, the server component does not store the provided document centrally at any time. Also, confidential and privacy sensitive data are not written to log-files or other similar output channels. Thus, even system administrators are unable to retrieve any confidential data about verified documents[9].

The presented signature verification tool has originally been developed for the Austrian e-Government infrastructure. Thus, the tool supports a variety of document and signature formats that are specific to the Austrian e-Government strategy. For instance, the tool supports the verification of the Austrian PDF signature format 'PDF-AS' (Knall, 2010) as well as various XML based documents such as Identity Links[10] (Hollosi and Karlinger, 2005) or electronic Criminal Record Certificates[11]. Besides that, the presented tool also supports various document and signature formats that are commonly used all over the world. This includes the Adobe PDF signature format (ISO, 2008) as well as S/MIME (Ramsdell, 2004) or CMS/PKCS#7 (Housley, 2004) based signatures. Due to its extensible design and broad range of already supported document and signature formats, the tool holds a high potential to improve electronic signature based solutions in various fields of application.

4. CONCLUSIONS

Signatures as means to express declaration of consent play an important role in daily life processes. This applies to traditional processes by using handwritten signatures as well as to online processes in the fields of e-Business or e-Government using their electronic equivalent. Electronic signatures provide the advantage of being technically verifiable and thus guaranteeing integrity and non-repudiation of origin in digital environments. In order to prove correctness and authenticity of applied signatures, appropriate verification

[7] Note that attacks are theoretically still feasible through a compromised web browser that displays faked verification results instead of those being returned by the verification tool. That is why a signed report is provided which can be downloaded in addition.

[8] Note that also client-side tools might require a working Internet connection, e.g. to retrieve mandatory information via LDAP.

[9] Note that users need to implicitly trust the verification tool, as they have no means to verify the correct implementation of privacy preservation mechanisms and to verify the compliance with the operator's privacy policies. However, this also applies to the implementation of verification mechanisms. Hence, signature verification tools need to be regarded as trusted third parties.

[10] The ‚Identity Link' is an important component in the Austrian e-Government, which unambiguously links the identity of a citizen with one or more electronic certificates.

[11] https://apps.egiz.gv.at/strafregister/

means need to be provided. Signature verification is no trivial task because several requirements must be taken into account. In Section 2, key requirements for the design and implementation of reliable signature verification tools have been identified.

In this paper we have presented a signature verification tool that meets all identified requirements. The introduced tool follows a central and web based approach hence meeting the requirements of security and usability. Additionally, the requirement of usability is addressed by providing a minimalistic and simple user interface hiding any technical or cryptographic details from the user. The architectural design of the tool follows a modular approach thus being able to support different signature and document formats. This fulfills the requirement of scalability.

The support of various signature and document formats within one single service defines an important feature because the electronic signature landscape is still quite heterogeneous at the moment. Although several initiatives for regulating the application of various signature formats exist, cross-border applicability remains an open issue though. Due to our modular architectural approach, new signature and document formats can easily be added and integrated in our signature verification tool and thus will not lock out any new formats coming up. Furthermore, sustainability and ease of use of our solution has already been proven by a production period of more than four years.

REFERENCES

ETSI, 2006. ETSI TS 101 903 – XML Advanced Electronic Signatures (XAdES).

ETSI, 2009. ETSI TS 102 778 - Electronic Signatures and Infrastructures (ESI);PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1.

European Union, 1999. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. *Official Journal of the European Communities*.

European Union, 2011. Commission Decision of February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. (2011/130/EU). *Official Journal of the European Union*.

Hollosi, A. and Karlinger, G., 2005. XML Definition der Personenbindung. Available from: http://www.buergerkarte.at/konzept/personenbindung/spezifikation/aktuell/

Housley, R. et al., 2002. IETF Standards Track RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Housley, R., 2004. IETF Standards Track RFC 3852 - Cryptographic Message Syntax (CMS).

ISO, 2008. Document management – Portable document format – Part: PDF 1.7.

Knall, T., 2010. PDF Signatur/Amtssignatur Spezifikation, version. 2.2. Available from: http://egovlabs.gv.at/docman/view.php/8/56/PDF-AS-Spezifikation-2.2.pdf

Pinkas et al., 2008. IETF Standards Track RFC 5126 - CMS Advances Electronic Signatures (CAdES).

Ramsdell, B., 2004. IETF Standards Track RFC 3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification.