Trusted Cloud

Trusted Cloud Competence Centre

Working paper – Modular Certification of Cloud Services

No. 4

Working party – Legal Framework for Cloud Computing

Cloud computing can only be economically successful in Germany if we frame enabling legislation for the efficient use of cloud services. It is therefore especially important to have a legal framework that favours innovation. This is why the Federal Ministry for Economic Affairs and Energy (BMWi) has established a separate working party for the legal aspects of cloud computing at the Trusted Cloud Competence Centre.

Together with project participants from the Trusted Cloud Programme, experts from business and industry, the legal profession and the scientific community along with representatives from data protection authorities in the working party, Legal Framework for Cloud Computing, prepare proposals for dealing with legal issues. It is headed by Prof. Dr Georg Borges. Priority topics include data protection, contractual arrangements, copyright, liability questions and criminal liability risks. In addition, a pilot project for the data protection certification of cloud services is being conducted to pave the way for the legally compliant use of cloud computing and an assured high standard of data protection.

Pilot project: Data Protection Certification for Cloud Services

Problem: Efficient data protection in cloud computing

When using cloud computing services, there is a need to assure adequate data protection that also includes secure outsourced data processing by the cloud service provider. An assessment must therefore be made of the technical and organisational measures it takes to ensure this. It would, however, be impracticable for every cloud service user to evaluate the technical systems of each cloud service provider and this would also incur excessive costs. Many companies wishing to avail themselves of cloud services cannot do this on their own.

Solution: Data protection certification for cloud services

These difficulties can be remedied with a suitable certification method that encompasses all legal data protection requirements for the contracted data processor in cloud computing, where its technical measures are reviewed by a professionally competent and independent certification agency. The findings of this evaluation will benefit all cloud service users. This certification can ensure both a high standard of data protection and lay the foundation for cloud service use.

Objective of pilot project

On behalf of the Federal Ministry for Economic Affairs and Energy (BMWi), the working party, Legal Framework for Cloud Computing, at the Trusted Cloud Competence Centre has drawn up a scheme for this kind of certification procedure, documented in its legal-policy position paper, Data Protection Solutions for Cloud Computing, dated October 2012. Based on this scheme, the pilot project, Data Protection Certification for Cloud Services, will draw up the details for the data protection certification of cloud services and carry out trial certifications for eligible individual cloud services.

Table of contents

1 Goals and challenges of cloud service certification

Aim of certification and current discussion

When using cloud computing services, there is a need to assure adequate data protection that also includes secure outsourced data processing by the cloud service provider. An assessment must therefore be made of the technical and organisational measures it takes to ensure this. Where the cloud service provider is engaged in outsourced data processing, the cloud service user (the recipient of the cloud service) is legally bound to satisfy itself that the technical and organisational measures taken by the cloud service provider meet regulatory requirements.

It is not, however, feasible for every cloud service user to check the technical systems of the cloud service provider. This would entail excessive costs (for multiple testing in some cases), could itself pose security risks and could not be carried out by many cloud service users on their own, particularly small enterprises.

These difficulties can be remedied with an appropriate certification method that encompasses all legal data protection requirements for the contracted data processor in cloud computing, where the technical measures of the cloud service provider are evaluated and confirmed by a professionally competent and independent agency. The findings of the test can be provided to all cloud service users and save them the trouble of conducting their own audit. This certification can both assure a high standard of data protection and lay the foundation for efficient cloud service use.

The working party, Legal Framework for Cloud Computing, has submitted a scheme for this kind of certification procedure and called for the legal regulation of certification under European data protection law to harmonise certification standards in the European single market (working party, Legal Framework for Cloud Computing: Legal Data Protection Solutions for Cloud Computing, Oct. 2012). A related legislative proposal has been drafted.

Though pursuant to the Federal Data Protection Act (BDSG), other initiatives, such as the standard drawn up by the German Association for Data Protection and Data Security and the Professional Association of German Data Protection Officers called Requirements for Processors under Section 11 of BDSG, are premised on certification as an efficient solution for guaranteeing the audit obligation in outsourced data processing.

In Article 39, the draft General Data Protection Regulation submitted by the EU Commission contains the normative basis for this kind of data protection compliance certification. The amendment to Article 39 proposed by the European Parliament's LIBE Committee is consistent with this aim. A draft for Article 39 prepared in the Council of Ministers with a new Article 39a even includes essential elements from the scheme submitted by the Legal Framework working party.

The pilot project, Data Protection Certification for Cloud Services, conducted by the Trusted Cloud Competence Centre will upgrade the scheme for data protection certification devised by the working party, Legal Framework for Cloud Computing, and try it out on selected examples.

In the following, we shall discuss the scheme devised in the Legal Framework working party's proposition paper, Data Protection Approaches for Cloud Computing, and the preconditions and impacts of certification.

Subject and scope of certification

The subject of certification derives from its aim. As certification is supposed to replace the need for the cloud service user as client to audit the processor's, i.e. the cloud service provider's, technical and organisational measures in cloud computing, the subject of certification must therefore be the service commissioned by the cloud service user, that is the service rendered to it by the cloud service provider.

From the German perspective, the scope of certification must accordingly encompass all aspects that have to be evaluated by the cloud service user as client in pursuance of Section 11 in conjunction with Section 9 of BDSG and in future possibly Article 26 of the General Data Protection Regulation. The prime concern is with measures for protection against unauthorised data processing.

Efficiency as a key challenge for certification

A procedure to achieve the cited aim of obviating the need for cloud service users to conduct their own audit of measures by relying on a certificate must find answers to several problems. For example, it must specify the verification requirements and certification procedure and demarcate responsibilities and competencies. The scheme devised by the working party, Legal Framework for Cloud Computing, calls for the future regulation of these aspects under law to lay a legally binding foundation for certification and the reliability of certificates.

Probably the foremost challenge in practice will be the possible substantial costs entailed in auditing and certifying data processing systems. There is a particular risk that excessive requirements and the related high costs for auditing and certification will make these unattractive for many, especially smaller, cloud service providers. In its proposed amendments (Article 39(1b) new) to the draft General Data Protection Regulation, the European Parliament rightly demands 'affordable' certifications.

A major structural problem for cost-effective auditing and certification, not least in cloud computing, consists in the subject of certification, which must pertain to the service commissioned by the cloud service user.

Cloud service providers offer many, different service packages (functions) to meet the specific needs of their clients. A basic concern of cloud computing is to provide users with data processing services they actually need. Their customised design for different user groups contribute to the cost advantages of cloud computing.

The many, different service options cloud service providers offer their clients poses a decisive problem for certification: As certification pertains in principle to the service commissioned by the client, each one of these various service options needs to be certified.

If each one of these service packages requires a separate audit, the provider would have to repeatedly bear all the costs for auditing and certification. This would make it much more difficult for cloud service providers to offer new products. Above all, this approach would be inefficient, as the individual components of the service packages would have to be assessed several, possibly multiple, times, although their technical application is identical.

To be effective then, certifications must guarantee a cost-effective, efficient system that avoids multiple audits.

2 Proposed solution: Efficient and cost-effective modular certification

A key element of certification in the scheme drawn up by the working party, Legal Framework for Cloud Computing, is that as far possible a service must only be tested once - by a competent and independent agency. This audit should be of benefit to all users of this service.

The same must apply within certification: The technical and organisational measures should only be assessed once and the audit should be valid for all fields of application, provided it comprises the relevant requirements for each.

This aim could be partly achieved by conducting a complete certification of all the provider's services. If the largest possible range of cloud services offered by a provider is audited and certified, the certificate must also comprise parts of overall service delivery. For example, if a cloud service provider offers services A, B and C and the services provided from this range have been audited and certified, including their interaction, this certificate will also apply for a service range consisting of services A and B.

Complete certification, however, has its limits and disadvantages. It does not answer the question of how to proceed when the cloud service provider would like to add a new component, D. Complete certification would also be disproportionately expensive, if, for example, a cloud service provider only wishes to have parts of his service range certified, because certification is relevant for these alone.

Data protection compliance certification therefore needs further development to be efficient: When alterations are made to service delivery, it should be possible to have recourse to previous certifications, so that only changes may need to be certified anew. Finally, it must be possible for each of the individual services, designated below as modules, to be audited and certified separately and make reference to this when certifying combinations of modules (services).

This approach, which can be designated as modular certification, will enable efficient certification and afford cloud service certification a broad field of application. In this modular form of certification, a distinction has to be drawn between horizontal and vertical modularisation.

3 Horizontal modular certification

Horizontal modularisation of data processing services

Modular certification caters for the fact that data processing services are often designed in a modular format. For example, data storage can be provided as a separate service, but also makes up part of almost all the more complex services. Email can be provided as a single service, but is often contained as a module (function, element) in service packages. Individual modules are frequently put to multiple use. A technically identical module, for instance, is provided as part of various services or service packages for different clientele. This is necessary as the only way to organise efficient service delivery to individual users.

As services are combined at application level, this can be accordingly termed the horizontal modularisation of data processing services (or applications).

Horizontal modularisation of auditing and certification

The horizontal modular architecture of services calls for horizontally modularised auditing and certification. Under the same test requirements, an email service, for example, should not have to be audited twice, because it is provided once as a service for consumers and again - technically identical - as a component of a service package for small enterprises.

4 Vertical modular certification

Vertical architecture of data processing services

A modular architecture is also discernible in the composition of the individual services. A data processing service is based on several respective technical and organisational constituents (components, elements). For example, a distinction must be made between devices and programmes. Equipment needed for a service, such as servers, are located in a server room. Relevant technical and organisational requirements apply for this and for technical infrastructure.

These basic technical resources, from the server room to power supply, etc. to programmes, can be split up systematically into levels or functions. As a general rule, an application is based on several levels that can be operated through various technical measures.

These technical components are often used by several applications alike. For example, a server room can be used for the majority of or even a multitude of systems that serve different applications or several applications or even virtual systems can be operated on one physical server.

Efficient auditing and certification of individual service components

Similar to the different combination of applications in various service packages, the question when certifying services is whether individual service components must each be subjected to a new evaluation, if they are deployed for another service. Must, for instance, the security of a server room be tested repeatedly, if a storage service is offered alongside an email service? Or, assuming the same requirements apply, would it not suffice for the server room to be checked once? Obviously, multiple auditing of the same technical and organisational arrangements for different services to the same test requirements, the security of server rooms, for example, would be inefficient.

The aim must therefore be to ensure that a test for an individual technical and organisational component applies for all the services where it is deployed, provided the audit comprises the normative requirements for the respective services. A certificate for an individual service must accordingly be able to draw on this kind of test. This can be designated as vertical auditing and certification.

5 Equivalence of modular certification

Modular auditing and certification can be equivalent to the uniform, separate certification of a service on offer, provided the modular certification comprises all features of the appropriate audit and certification and meets the same requirements for the relevant elements as uniform, separate audit and certification.

This must meet demanding criteria. For instance, the outcome of a modular audit must comprise all test requirements for the respective service. Moreover, all audits to which the service certificate refers must also be carried out to a uniform procedural standard that meets the requirements for the proper evaluation of the respective service. No disadvantage should arise for a third party as compared with a uniform audit and certification with respect to responsibility and liability.

If these prerequisites have been met, a certificate based on modular auditing is equivalent to one based on a uniform test and must be accorded the same substantive and legal status.

6 Elements and challenges of a modular certification system

Relationship between audit and certification

In a system of modular certification, the relationship between auditing and certification has to be clarified. Systemically, testing and certification are definitely separate procedures, but not necessarily in organisational terms. The audit is an examination carried out by a person, auditor or auditing agency to ascertain whether the test object has the requisite normative features (meets test requirements). Certification is the confirmation by a person, a certification agency, that the audit has been conducted (properly) by the auditor. The same person can conduct the audit and certification, but these can also be separate organisational and legal entities.

Modular certification with reference to certificates

In modular certification, there is nothing fundamentally special about the audit. A test must be carried out of the technical and organisational requirements for a module or component. A certificate should be able to be issued for each audit. It is essential for modular certification that reference can be made to (previous) examinations of the modules or components, particularly if the audit is documented by a certificate. Reference is therefore then made to a certificate.

In modular certification, each service provided to a user requires a certificate. This can consist in part or in full of the reference to various certificates issued for the individual components and modules.

For example, a certificate for a service package made up of modules A, B and C could refer to existing certificates for the modules A and B and be based on an additional audit conducted as part of the certification for module C and the interaction among the three modules. Alternatively, it could refer to valid certificates for all three modules and the interaction among them. Equally, a certificate for a module A can be made up of existing certificates for components 1, 2 and 3 and an additional audit conducted as part of certification of the interaction among the components.

Relationship among audit, certification and responsibilities

In a system of modular certification, certificates can be based on the audits and certifications of various certification agencies. It may, for example, be possible for a computer centre to be certified by certification agency A, while the service performed using the computer centre is certified by certification agency B.

The prerequisite for a combination of certificates from different certification agencies is that the audit by the certification agency to whose certificate reference is made is equivalent to that of the other agency. This is the case if the audit is carried out applying at least equivalent audit requirements and the certification procedure in which the certificate has been issued also meets the requirements of the certification procedure in which reference is made to the previous certificate. This calls for complete transparency of the audit requirements and the ability to ascertain the equivalence of the certification procedure.

This kind of combination of certificates from different certification agencies gives rise to questions of responsibility and liability that need further consideration. Regardless of this, however, reference to certificates of other certification agencies is possible, provided the audit conducted there is equivalent to that of the other certification agency.

A cornerstone of a system of modular certification is therefore the transparency and legal certainty of test requirements and the equivalence of audits.

7 Application fields of modular certification and cloud computing

The issues involved in the modular certification of data protection are not just confined to cloud computing; they apply generally to all data processing services.

Certification as such and equally its modular form does not just play a major role in outsourced data processing. It is of special benefit here, since it enables the client (cloud service user) to have confidence in the certificate and obviates the need for it to conduct its own audit of the technical and organisational measures taken by the processor. Certifications are also important beyond this. For example, a certificate can also be relevant for the admissibility of data transmission, in the case of function transmission, for example. Moreover, it can also have a bearing on the liability of the management of a data-processing company that applies certification to meet its obligation to monitor the legality of data processing (compliance).

The concept of modular certification is, however, particularly relevant for cloud computing, as the modularisation of data processing service delivery is a characteristic feature of cloud computing as a dynamic service tailored to the needs of the cloud service user, which nevertheless typically consists of standard elements. Cloud computing is therefore rightly viewed as the primary application case for developing modular certification.

8 Conclusion

The aim of enabling cost-effective and efficient data protection certification for cloud services can be achieved with a system of modular certification that permits both the horizontal and vertical inclusion of previous certifications. This dispenses in general with the need to re-examine already certified elements.

At application level, horizontal modularisation of certification enables a certificate to be issued for a majority of modules (applications) so that previous, valid certificates for individual modules can be incorporated by reference in the certification. Vertical certification modularisation enables reference to be made to current certificates for the different technical and organisational components when certifying an individual application and include these in certification.

Modular auditing and certification can be equivalent to the uniform, separate certification of a service, provided the modular certification comprises all features of the requisite audit and certification and these are of the same quality.

Authors

Oliver Berthold, Berlin Commissioner for Data Protection and Freedom of Information

Prof. Dr Georg Borges, Trusted Cloud Competence Centre

Mathias Cellarius, SAP AG

Susanne Dehmel, BITKOM

Thomas Doms, TÜV TRUST IT GmbH Unternehmensgruppe TÜV Austria

Publishing details

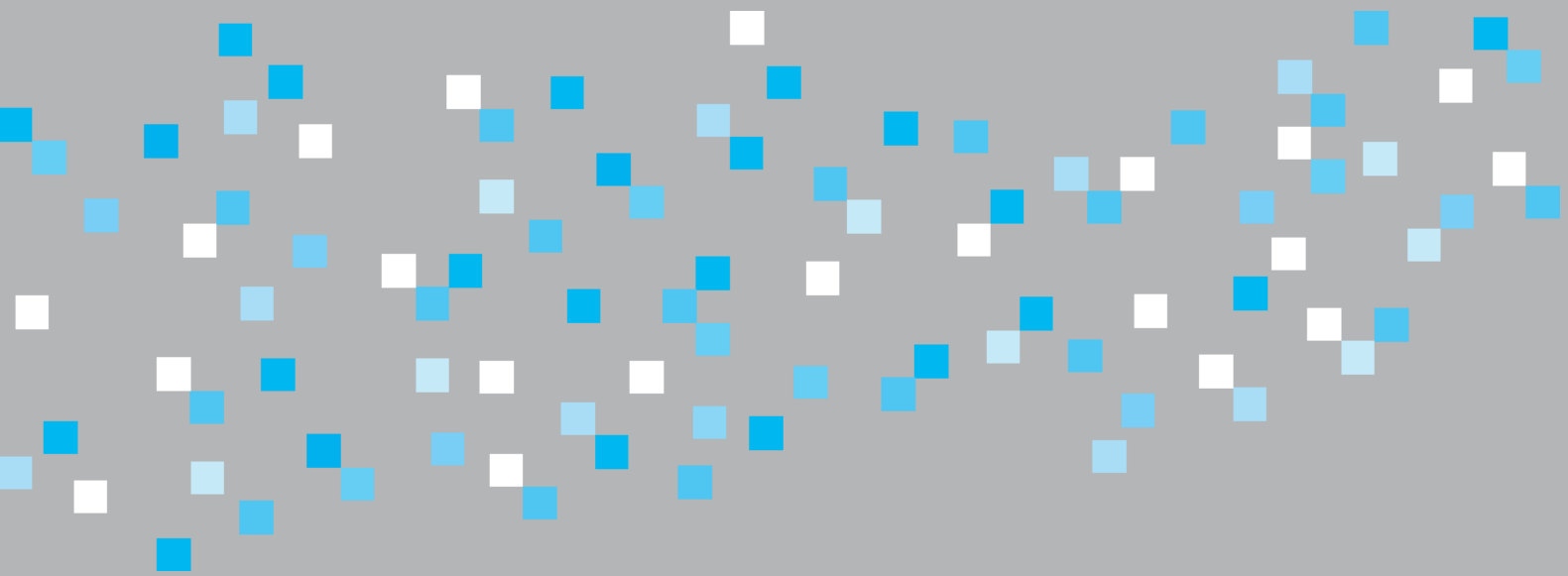
Published by
Trusted Cloud Competence Centre
Working group: Legal Framework for Cloud Computing
E-Mail: kompetenzzentrum@trusted-cloud.de
www.trusted-cloud.de

On behalf of the Federal Ministry for Economic Affairs and Energy (BMWi)

Design
A&B One Kommunikationsagentur, Berlin

Printed by
DCM Druck Center Meckenheim

As at: March 2014



www.trusted-cloud.de