TÜVIT

Trust Services in the Cloud

...and what does it mean for conformity assessment?

Matthias Wiedenhorst | CA-Day 2023 | 12.10.2023

Motivation

- More and more conformity assessment requests from TSPs and TSP component providers, where the service or relevant parts of it are operated in the cloud
- Uncertainties in how to properly handle such conformity assessments
- Unharmonized way of performing such conformity assessments

Scoping

- Different models available, typical is „Infrastructure as a Service / IaaS“
  - Provision of virtualized computing, storage, network and connectivity by Cloud Service Provider (CSP)

- Not relevant for this presentation:
  - Using clouds as “content delivery network”, e.g., for signed revocation information
  - Using clouds as storage for encrypted data / backups only

- Some services, e.g., “Remote Signing Services / QSCD Management on behalf”
  - Are a cloud service from the viewpoint of the customer
  - But of course, not necessarily from the viewpoint of service operation

Basic approach

- For the conformity assessment, just ignore the Cloud Service and treat it identical as if it would be physical hardware operated by the TSP itself.
- ...?
  - I guess we are all on the same page that this cannot be an option...
- For the conformity assessment, just verify that the CSP is certified according to [ISO27001 | ISO27017 | ISO27701 | ...]
- ...?
  - This is better... But is that enough?

Basic approach

- ISO 27xxx does not define a certain „security level“.
  - It is about a management system that needs to define its individual security requirements based on risk assessment
    - For a QTSP such risk assessment will result in high security requirements
    - For a CSP usually targeting the masses of “average IT companies”...?

- NIS2 and the ETSI norms, especially ETSI EN 319 401 include a large number of explicit requirements regarding general IT security for trust service providers
  - A certification according to ISO 27001 does not guarantee that any of these are fulfilled...

ENISA report

- Mid-2023, ENISA published a report regarding the use of cloud services by trust service providers
  - Comparison of general CSP standards (here: ISO 27017) against TSP requirements
  - Results of a survey performed with a large number of stakeholders in the TSP sector
  - Implications for conformity assessments

TÜVIT

ENISA report

- Comparison of general CSP standards against the ETSI EN policy requirements for TSPs
  - „Most of the aspects of these policy requirements are likely to be met by CSPs […]“
  - “Nevertheless, before this can be confirmed, detailed checks on provisions of a particular CSP against the ETSI policy requirements are required.”
  - “The use of cryptographic services and HSMs require particular attention.”
  - “Thus, it is not considered that [Remote Signing Service / Remote QSCD] could be provided by a CSP […]”

TÜVIT

ENISA report

- Results of a survey performed with a large number of stakeholders in the TSP sector
  - 89% of the questioned CABs answered, that only a documentary review of CSP is not sufficient
  - 89% of the questioned CABs answered, that they believe the terms and conditions of CSP do not contain adequate clauses allowing access for auditors to perform TSP assessments
  - Only 25% of the questioned CSP stated that a TSP's conformity assessment body would be allowed to perform additional, necessary audit activity

    => 75% would not…
  - 39% of SBs answered that they have experience with TSPs use of the cloud, but only 6% answered, that it is something they would promote

TÜVIT

ENISA report

- Implications for conformity assessments and Conclusions

  - “This will require the TSP to provide evidence that requirements of the services of the CSP, on which the TSP depends, are met for example by the CSP through certifications with more detailed information as considered necessary by the auditor.”
  - “However, there is still the problem that the assessment of the controls that the TSP has contractually outsourced to the cloud provider can only be done in a documentary manner, which reduces the quality of the audit.”
  - “While some impediments from the audit perspective exist, the survey results have shown that CABs can already perform audits on many trust services.

TÜVIT

ENISA report

- Implications for conformity assessments and Conclusions
  - “This will red… quirements of the services of t… met for example by the CSP thro… rmation as considered necess… auditor.”
  - “However, there is … the problem that the assessment of the controls that the TSP has contractually outsourced to the cloud provider can only be done in a documentary manner, which reduces the quality of the audit.”
  - “While some impediments from th… results have shown that CABs ca… services

89% of CABs answered, that this is not sufficient...

An assessment with lower quality for a scenario with an increased risk...?

TÜVIT

Perspective of a CAB

- ISO/IEC 17065:2012 – “Conformity assessment – Requirements for bodies certifying products, processes and services”
  - Section 7.4.5: “The certification body shall only rely on evaluation results related to certification completed prior to the application for certification, where it takes responsibility for the results and satisfies itself that the body that performed the evaluation fulfils the requirements contained in 6.2.2 and those specified by the certification scheme.”

- CAB must evaluate whether the CSP fulfils all relevant requirements, but can do this only through relying on external assessment results

- CAB must take full responsibility for external results that he decides to accept as part of his conformity assessment

Problem summary

- Existing standards / certifications of CSP do not cover the specific requirements for QTSP
- Individual evaluation of the specific requirements for each TSP using a CSP necessary
  - In many cases only possible based on existing certification documentation, which includes only very limited information regarding such details
- In practice this might lead to the “Basic approach” being applied by CABs

Possible solution

- Define a certification scheme for CSP that is explicitly regarded as appropriate for qualified trust service providers
  - EUCS – European Union Cybersecurity Certification Scheme on Cloud Services
  - Will define different levels of assurance
  - EUCS might become an appropriate scheme?

- Addition of an ETSI EN 319 401 requirement, stating that if the TSP outsources to a CSP, the CSP shall be certified according to that scheme.
  - CAB must not evaluate (and decide) on its own whether a certain scheme is appropriate
  - Task would not be any more to evaluate whether the CSP fulfils all relevant requirements (through relying on external assessment results) but to verify the existence of a proper certification

TÜVIT

Thank you very much!

Matthias Wiedenhorst
Head of Certification Division TSP

TÜV Informationstechnik GmbH
m.wiedenhorst@tuvit.de