October 2013

Cloud Security Whitepaper

A Briefing on Cloud Security Challenges and Opportunities

SINTEF ICT | Software Engineering, Safety and Security
Martin Gilje Jaatun, Per Håkon Meland, Karin Bernsmed

Telenor Research
Humberto Castejón, Astrid Undheim

EXECUTIVE SUMMARY

Cloud computing has emerged as a major shift in how computing resources are deployed and consumed, both by individuals and enterprises. However, despite benefits such as reduced up-front investment, lower costs and more eco-friendly operation, a large proportion of potential cloud customers are voicing misgivings with respect to how security and privacy are handled in the cloud. This distrust has been further fueled by media events, such as the PRISM scandal, which really shows how difficult it can be to know to what extent our data is being monitored for legitimate or illegitimate purposes.

When moving to the cloud, a security cautious customer would typically worry about issues such as:

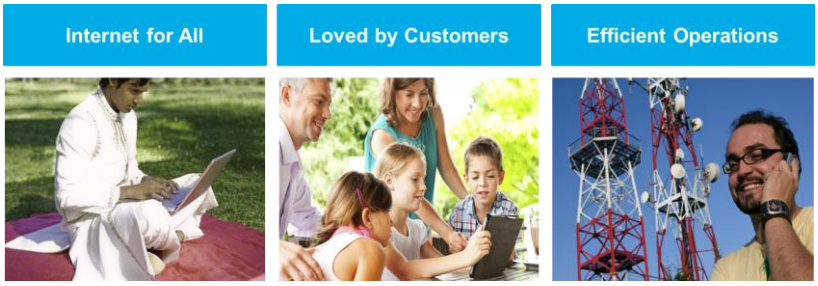
- How will security be handled and who will be responsible for what?
- Which certificates and standards are best for cloud security?
- Where should I look to find a service that fulfills my security needs?
- How can I compare the security level of two otherwise equal services?
- What kinds of security guarantees should be included in the contract?

Alas, it is usually very difficult and time consuming to find good answers to these. This is often due to either lack of documentation or reluctance from the providers to give specific promises to individual consumers. In order to aid potential cloud customers, CloudSec—a joint research project between Telenor and SINTEF—has created a checklist for cloud security, which provides a systematic approach to what kind of cloud-specific questions a customer should seek answers to. This checklist can both help to evaluate a single provider's security stance, and will also make it easier to compare the security of alternative cloud providers.

This whitepaper provides a brief introduction to the cloud ecosystem, and explains cloud security challenges and opportunities based on our checklist. We further elaborate on the role of security in cloud service contracts.

Telenor's strategic ambitions are threefold: be loved by customers, be a cost-efficient operator, and bring Internet to all. Telenor's embracement of cloud technology directly supports the first two ambitions. Use of cloud technology for internal operations and support systems is directly answering the cost-efficiency ambition, while adopting cloud technology for delivering new and innovative services to customers is a necessary step in order to stay relevant and be loved by customers, as the mode of service production and consumption is shifting.

In contrast to only a few years ago, Telenor is nowadays using cloud technology and services more and more frequently for internal operations and production of own services, as well as a source of revenue, through the Tapstorm initiative. The security checklist discussed in this whitepaper has been tested in several of these initiatives.



THE CLOUD ECOSYSTEM: WHO IS WHO

The characteristics of cloud services include on-demand self-service, broad network access, resource pooling, rapid elasticity and measured services. There are three main types of service models; namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Services can be deployed into public clouds, private clouds or hybrid clouds. The combination of the different service and deployment models enables different business models with new business roles. The cloud ecosystem will thus include a number of players that will choose to take on those roles depending on their position in the market and their business strategy. The four most prominent roles in the cloud ecosystem are:

Cloud computing enables different business models, all of which are of relevance for Telenor

The **cloud customer** maintains a business relationship with one or more cloud providers and uses services from one or more cloud providers (the latter set of providers need not overlap completely with the former). The cloud customer may also have their own individual end-users, which could be employees or other customers who are using the services that they procure.

The **cloud provider** makes cloud services available to interested parties. This includes providing the services, arranging for networked access to the cloud customer and, for IaaS providers, acquiring and managing the computing infrastructure.

The **cloud broker** (sometimes called integrator or reseller) is someone who manages the use, performance, and delivery of someone else's services. A cloud broker will identify, integrate and customize cloud services in accordance to the customers' needs and may also be able to negotiate the relationships between the customer and the provider. Even if it is not common today, the cloud broker is foreseen to take an important role in the future cloud ecosystem. Telenor is already pursuing this position through the Tapstorm brand, initially being a cloud broker for business SaaS applications.

The **cloud carrier** acts as an intermediary that provides connectivity and transport of cloud services between cloud customer and cloud providers. Cloud carriers provide access to customers through different network access and devices.

Telenor has already adopted several roles in the cloud ecosystem:

- *Internal cloud provider*. Telenor's Global IT initiative uses private cloud solutions for improving internal operations.
- *Cloud customer.* Telenor Comoyo uses public cloud services from Amazon for agile and cost-efficient deployment of services and platforms.
- *Cloud broker*. Tapstorm acts as a cloud broker providing 3rd party cloud services to Telenor's customers. It is a source of revenue and stickiness.

CLOUD COMPUTING SECURITY CHALLENGES

Cloud computing security can be viewed as a double-edged sword, which is reflected in the attitudes of organizations that are using cloud services today or that are planning a migration in the near future. Security is often stated as a major concern amongst cloud customers, mostly due to difficulties of getting necessary contractual guarantees of data control (in particular data handling in accordance to existing legislation), availability concerns, the potential risks of data loss and the difficulties of enforcing the organization's security policies. On the other hand, some organizations think that the adoption of cloud services has increased their organization's IT security. Clearly, there are both challenges and opportunities with the cloud.

Cloud computing security can be viewed as a double-edged sword

The standard offerings from cloud providers are high-volume low-cost services that run on shared infrastructures. Cloud contracts are therefore often based on the provider's standard terms and conditions and many cloud customers report on difficulties when attempting to negotiate the contract terms[1]. Services are offered on a take-it or leave-it basis and most customers simply lack the power of bargaining. The ability to negotiate cloud contracts also depends of the type of service offered. SaaS services are usually offered as-is, without any room for negotiation, whereas the provider can be more willing to negotiate an IaaS service offering, in particular when the customers are buying large amounts of storage or processing capabilities. A general observation is that contract negotiations (if any) can take a substantial amount of time, and the contract terms tend to be vague. Unfortunately, the standardization work on cloud contracts is still very much immature, for instance, there is no well-defined terminology or mandatory obligations, and this makes it difficult to compare contract offerings in an easy way.

Services are offered on a take-it or leave-it basis and most customers simply lack the power of bargaining.

The CloudSec project, which is a research collaboration agreement between Telenor and SINTEF, has developed a cloud security checklist that contains important security obligations that any organization should take into consideration when dealing with cloud services. The checklist is divided into seven categories and forty areas, and contains concrete advice to check for within each area. These advices are based on work from NIST, Cloud Security Alliance, FedRAMP and ENISA, as well as on ongoing research and development for cloud security, and it has been tailored to be hands-on and intuitive to use. Telenor has used the checklist for auditing of the Tapstorm platform and for the Global ERP HR RFQ process. The checklist will be used in the following sections to describe and systemize security challenges related to cloud computing.

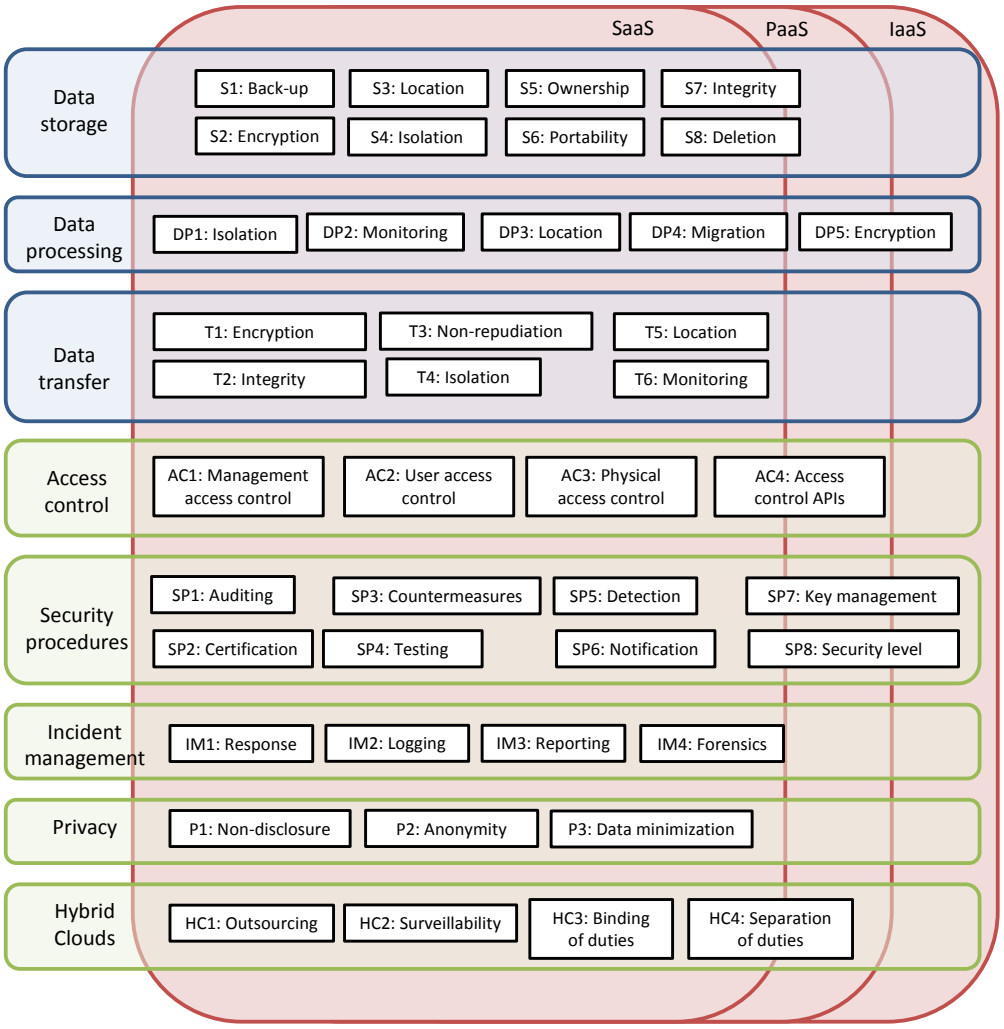


Figure 1: Cloud Security Checklist Framework

OWNERSHIP OF CUSTOMER DATA

When data resides in a cloud data center, it is important to clarify the ownership rights. There has been some concern that many providers' terms of use could appear to give providers intellectual property rights to the information they store or process, but studies by legal experts have found no evidence of this[2]. However it is still important to clarify what rights—if any—are conferred on a cloud provider and what this means in practice (S5: Ownership). Encryption is one way to protect data that is being stored; however, this is not very useful when the data needs to be processed in the cloud[3]. The customer should therefore make sure that data ownership is clearly defined and that the agreed terms are acceptable with respect to the customer's own security policy. It is also wise to clarify the ownership of data that is generated when the customer uses the service, such as trace logs, service usage patterns, Quality of Service information, and the like.

When data resides in a cloud data center, it's important to clarify the ownership rights

USAGE OF CUSTOMER DATA

Having clarified the ownership of customer data, it is equally important to control how providers can use the data (P1: Non-disclosure). An example is Microsoft's security, privacy and compliance information for O365 where it is stated that the address book data for Office 365 Small Business customers is used for marketing purposes[4].

DELETION OF CUSTOMER DATA

Cloud services are by nature virtualized and duplicated, which is good for ensuring uptime and availability. Furthermore, the duplication is compounded by conventional backup processes performed in each data center. However, when the owner of a particular dataset wishes to delete it (S8: Deletion), this wide data distribution becomes a major challenge. It is difficult enough to ensure that all duplicated copies in each datacenter are erased, but ensuring that all backup media is expunged as well can take months. It is important to be aware that "deletion" does not always mean that data is actually erased; it is often only the pointers that indicate where the data fragments are located that are erased. Data deletion will therefore in most cases not be guaranteed by providers beyond what is performed in a normal overwriting cycle of backup media. Provider commitments with respect to data deletion are important for cloud customers; not only when they are using the cloud service, but also after the contract has been terminated.

It's important to be aware that "deletion" does not always mean that data is actually erased

FOG COMPUTING

In the more recent "old days", one would buy a cloud service from a single cloud provider and that was it. However, the cloud ecosystem has evolved into a more diffuse fog of several cloud providers, resulting in less security visibility. A cloud service is likely to have many layers of abstraction that build on top of each other. Service providers adapt and compose several services into one, which is then offered to the cloud customers. Software-as-a-Service (SaaS) applications that an end-user interacts with are already often based on other providers' PaaS solutions, which in turn often run on yet other providers' IaaS offerings (HC1: Outsourcing). Numerous combinations exist and more are expected to come. There will be chains of services and providers involved in the final service delivery. An example is Comoyo Capture, which is based on DropBox, which in turn is running on top of Amazon WS.

From a security point of view this means that the cloud customer may, sometimes unknowingly, rely on many different parties, hence being subject to multiple points of failures, an increased attack surface and difficulties in verifying that legislation and internal security policies are being adhered to.

Many of the security challenges in cloud computing are in part related to the complex provider supply chains in this ecosystem. To complicate things even further, services and data may be replicated horizontally among multiple providers. As a consequence, it is often extremely difficult to determine where data is being stored or processed at any one time.

Many of the security challenges in cloud computing are related to complex provider supply chains

ACCESS CONTROL

Access control management (AC2: User access control) can be challenging enough within a single organization, but when moving services and data to the cloud, a new dimension is added. Cloud customers often fear unauthorized access to their data. Most providers have "backdoors" to their customers' data, and they often reserve the right to access it for maintenance, support and service reasons. It can be very difficult to know which roles and people have access to your data from the cloud provider side. For instance with Office365, database administrators employed at Microsoft reserve the right to have access to all the resources in all their databases, including their customers' data. Additionally, the Microsoft Operations Response Team and their support organization can access this data as well.

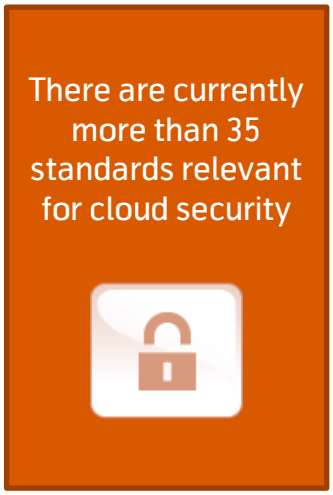
MONITORING AND AUDITING

Cloud providers may offer various options of monitoring data and processes related to their services; both from the provider's perspective of ensuring acceptable use, and from the customer's perspective of keeping track of what is happening in their corner of the cloud. This could include monitoring virtual machines in IaaS or monitoring behavior of running applications in PaaS and SaaS (DP2: Monitoring). Another example could be monitoring of network communication between virtual machines by network-based intrusion detection systems (T6: Monitoring).

The big cloud providers have thousands, if not millions, of customers, and it would not be viable to allow any demanding customer to inspect a cloud datacenter as part of a service contract negotiation. Furthermore, due to the large number of other customers, allowing one customer unrestricted access to network and process monitoring data could jeopardize the confidentiality of other customers' data. However, many customers want to maintain a certain level of control, and some sectors are even required to do this by local regulations. Some of the smaller providers allow their customers to perform such on-site inspections as part of negotiation or annual reviews. In addition, accredited auditors may perform independent audits of cloud providers and their datacenters (SP1: Auditing).

STANDARDS AND CERTIFICATION

Many customers rely on security standards as a way to ensure that an adequate level of security is attained; however, there is not yet any established standard that will fit all cases. There are currently more than 35 standards relevant for cloud security and it is unrealistic to expect a cloud customer to be conversant with all of them. Many cloud providers will typically claim that they are compliant or certified to a certain standard, but the ground work here for the customer is to make sure that this is of relevance to the kind of security they are looking for (SP2: Certification). Upcoming standards such as *ISO/IEC WD 27017 Code of practice for information security controls for cloud computing* and *ISO/IEC CD 27018 Code of practice for data protection controls for public cloud computing services* are expected to be completed late 2013, but with the rapid development of cloud technologies and the slow standardization progress, they might be outdated after just a short while.



SECURITY TESTING

With traditional software installed in your own premises it is not uncommon to run security tests in a controlled environment. When services are deployed in a public cloud, organizations tend to lose this possibility since many cloud providers do not allow their

customers to do any testing on their own. Therefore, a typical check is to obtain information about the kind of security tests (SP4: Testing) performed, and what are the results.

INCIDENT MANAGEMENT AND RISK OF DATA LOSS

There is no such thing as a perfectly secure system, and incidents are bound to happen from time to time. What is important to check is how incidents are dealt with, in the preparation (SP1: Auditing), detection (SP5: Detection), reaction (SP3: Countermeasures, IM1: Response) and investigation phases (IM4: Forensics). In many cases it is up to the cloud provider to define *what* a security incident is, *when* or even *if* the costumers need to be informed about a breach, and *how* to notify them (S6: Notification). Recent events[5] have shown that providers often tend to keep quiet about security incidents for as long as they can, even though it is in the customers' interest to get informed as soon as possible.

In Europe it is expected that the new European Data protection framework, which is currently under a major revision, will include new obligations related to incident notification. This means that any cloud provider must establish mechanisms to notify regulators and affected companies and individuals of data breaches or information security incidents. The Cloud Security Alliance has recently released a whitepaper [6] on the necessity for forensic functionality as a part of the Service Level Agreements (SLAs), such as requirements for notification, identification, preservation, and access to potential evidence sources.

LOCK-IN AND PORTABILITY

Today, many up-and-coming cloud providers are not making money due to the effort and investment required to gain a sustainable market share. Some are bound to be put out of business and we will probably see many new competitors entering the scene as well. An unstable market is to be expected in the coming years as the cloud ecosystem grows into adulthood, so before deciding on a cloud service provider, it is important to have an idea on how to migrate to a different cloud provider should it be necessary (S6: Portability). Data lock-in is one of the top concerns organizations have towards cloud computing. The typical checks here are related to how much time one has to migrate the data, whether there are any tools or APIs for exporting the data, the format which the data will be recovered into, and how the original data is going to be deleted. For instance with an Office365 service you have 90 days to export your data, and it is the responsibility of the customer to do this himself. For file storage services, format is usually not a problem, but for SaaS it can be difficult to get the data out in a usable format. Using Office365 as an example again, Exchange Online data, including emails, calendar appointments, contacts, and tasks, can be downloaded to a local computer via export wizards, but that does not necessarily mean that the data can be imported into other email services.

ISSUES WITH REGULATION

Actors who have to abide by the European Data Protection Directive (DPD)[7] have to be conscious about whether they store personal data in the cloud, and if so, where that data is transferred (S3: Location). The directive prohibits transferring of personal data to jurisdictions that do not offer sufficient protection of such data, but determining which countries it would be OK to transfer data to is not something that is easily accomplished by the average cloud customer. Thus, the short-term solution for many European cloud customers is to request that their data—including back-ups (S1) and logs (IM2)—be stored only in European data centers[8]. However, even when a cloud provider agrees to such terms, it may not be easy to

Cloud customers that transfer personal data to the cloud will become data controllers and thereby need to follow strict requirements when engaging cloud providers to process the data

ensure that no undesired data transfers take place. This is again due to the complex provider chain, for instance where one cloud provider, whose datacenters are all in Europe, somewhere down the line uses services from another cloud provider that also has datacenters in India (C1: Outsourcing). It is currently difficult to verify data export restrictions in long cloud provider chains.

Another issue with regulation is related to the definition of "data controllers" and "data processors" in the DPD. Cloud customers who transfer personal data to cloud infrastructures will become data controllers and will thereby need to follow strict requirements when engaging cloud providers to process the data. The definition of "processing" in the DPD is very broad and includes any operation on data in a cloud infrastructure, including collection, storage or disclosure. In most cases, storage providers (IaaS) do not have any way to control what kind of data their customers upload to their data centers. They therefore risk becoming data processors (involuntarily and possibly also unknowingly), and thereby subject to the strict DPD regime, if their customers upload personal data to their data centers[9]. A "data processor agreement" must therefore always be established between the cloud customer and the cloud provider before personal data is transferred to the cloud.

Note that other regulations may apply in other jurisdictions and it is important for customers and providers to consider which rules pertain to them.

BRING YOUR OWN DEVICE (AND CLOUD)

"Bring your own device" (BYOD) poses an increased risk to many organizations, and is in many security circles referred to as "bring your own disaster". It means that employees use their own devices—such as smartphones and tablets—to access and store corporate information side by side with their own applications. BYOD raises a number of data protection concerns, mostly due to the fact that the device is owned by the user, but it is used to process personal data for which the organization is responsible. The problems with BYOD are now compounded by something we can call "Bring Your Own Cloud" (BYOC), which is considered an even bigger security threat[10]

BYOC introduces additional security threats to the organizations

With BYOC (soon to be referred to as "bring your own catastrophe"), employees are installing public cloud services such as Dropbox and iCloud on their corporate desktops and mobile devices. BYOC introduces additional security threats to the organizations, not only by exposing them to additional vulnerabilities that may be introduced by the software, but also by blurring the boundaries between personal data and business confidential data, hence making it difficult for the organizations to maintain and control their security policy for access and distribution of corporate information (HC1: Outsourcing).

CLOUD COMPUTING OPPORTUNITIES

Assuming organizations can manage the risks associated with the cloud, there are also some major security benefits associated with cloud computing.

In 2015 **10%** of the overall IT security enterprise product capabilities will be delivered in the cloud

LEAVE IT TO THE EXPERTS

Although many individuals may be uneasy about putting their confidential data into this faceless nebulous entity known as the cloud, the reality is that a cloud provider will generally have vastly better security procedures, physical protection, and not at least security expertise than any small or medium-sized enterprise (SME). For an SME, security tasks are most frequently handled by system administrators that have many other responsibilities, and security needs must compete with all the other mundane demands involved with keeping a system up and running. Due to economies of scale, a cloud provider can have a dedicated team of security specialists and cloud datacenters have physical protection on par with military installations.

A cloud provider will generally have vastly better security procedures, physical protection, and not least security expertise than any SME

Centralized data management also has its benefits—provided that one can manage the risk of data losses, portability issues, etc. Laptops and back-up disks are easily stolen, lost or broken. Adopting a thin-client concept, where most of the data is stored and processed in the cloud, will greatly reduce this risk. Also, centralized data storage is easier for a cloud provider to monitor and control, than it is for a system administrator in an SME to cope with a huge number of locally managed servers and workstations.

THIRD PARTY ASSURANCE

With the new European data regulation, cloud providers are subject to mandatory security audits (from 2016), adding another layer of assurance for customers, who also reap the cost benefits and easy eco-conscience[11] that come from using a cloud service.

SECURITY AS A SERVICE

Security can also be delivered as a service from the cloud. The most common examples are secure email and security web gateways, remote vulnerability assessment, and identity and access management solutions. According to Gartner, the high demand for such services is caused by the customers' lack of staff with the necessary skills, as a way to reduce costs or as a way to comply with security regulations quickly[12]. Gartner also expects that by 2015, 10 percent of the overall IT security enterprise product capabilities will be delivered in the cloud.

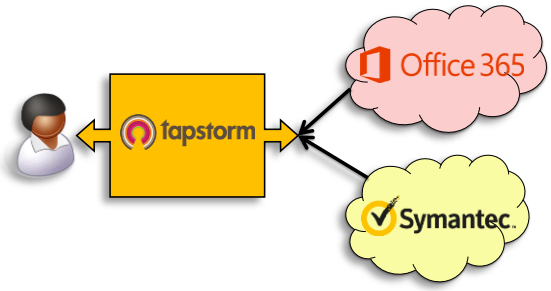
Cloud computing brings new business opportunities to Telenor as exemplified by the **Tapstorm initiative.**

Telenor has adopted a cloud broker role through the Tapstorm business division in Telenor Digital, providing a one-stop shop for 3rd party cloud services. Telenor, as a broker, can differentiate the delivered cloud services by bundling them with network services, and providing end-to-end security and a single SLA, as compared to two separate SLAs—one for the cloud service itself, and another for the network service.

Currently, Tapstorm offers 3rd party SaaS services, including Microsoft Office 365 and other solutions for email, web, backup and security.

In Tapstorm, delivering cloud services to business customers in a secure way, and properly handling and protecting the customers' data, is considered an important aspect of its daily business and is taken seriously.

That is why Tapstorm used the CloudSec checklist to perform a security audit of its cloud broker platform. The checklist proved to be helpful for doing a systematic analysis of the security risks with the chosen platform.



SECURITY IN CLOUD CONTRACTS

The relationships between the different entities in the cloud ecosystem are regulated by contracts, which—amongst other things—specify the customers' right to use the service, the terms of use, payment obligations, SLAs, data protection guarantees and the customers' termination rights.

Very few standard offerings contain security and privacy guarantees, except for basic data protection guarantees, such as whether—and how—stored data will be encrypted, what kind of authentication and access control mechanisms are in place, what kind of certificates the provider holds and sometimes also information on what geographic region the data centers are located in.

It is very rare that contracts include anything related to the provider's responsibility in case of data losses, any kind of proofs that data will be deleted when the service expires, the customers' right to do on-site audits on demand, or the right to do security, vulnerability and penetration testing[13]. Very few providers are willing to negotiate their standard offerings—at least not for SaaS and PaaS offerings. However, large customers may be able to negotiate a higher security level, in particular when they are buying infrastructure services (IaaS).

It is very rare that contracts include anything related to the provider's responsibility in case of data losses, any kind of proofs that data will be deleted when the service expires, the customers' right to do on-site audits on demand, or the right to do security, vulnerability and penetration testing

Note that standardization of cloud contracts is one of the core new elements of the upcoming data protection framework from the EU, but it is uncertain how much security will be included in these.

Since many different entities can be involved in the provision of a single cloud service, there are often chains of contracts between the different entities involved. Our checklist is intended to serve as a guideline during contract negotiation, and even if most of the checks are based on security controls that the primary service provider would be responsible for, we have also included additional checks that are applicable to so called "hybrid clouds", or clouds-of-clouds (HC1: Outsourcing, HC2: Surveillability, HC3: Binding of duties, HC4: Separation of duties).

CONCLUSIONS AND WAY AHEAD

Through examples, we have illustrated how the CloudSec checklist covers a majority of cloud security concerns experienced by potential cloud customers. The full CloudSec checklist can be used as a competitive advantage when marketing cloud services, by tailoring an offering more closely to the customer's needs. It can also be used in a more general setting, for customers to compare the security of competing offerings.

It is expected that the new European Data protection framework, which is currently under a major revision, will include new obligations related to incident notification, security audits, deletion and contract standards.

This means that any cloud provider must establish mechanisms to notify regulators and affected companies and individuals of data breaches or information security incidents. There will be more strict requirements for having regular security checks and how data is deleted (including logs, back-ups and aggregated data).

The new data protection framework is scheduled to be ready for adoption by 2014 and enforced from 2016.

Telenor is nowadays using cloud technology and services more and more frequently for internal operations and production of own services. Cost-efficiency, short time-to-market and business agility are the main factors for this.

Cloud technology is thus increasingly used in new IT initiatives within the Telenor Group, and is especially well suited for cross-border initiatives such as IT Shared Services. SaaS solutions are also increasingly being adopted at both the Group level and by the individual business units.

Examples are the ERP HR solution from Workday and the e-learning platform, which both are delivered as SaaS across the whole Telenor Group. IaaS solutions are also used by Comoyo for hosting Telenor's Global Backend, and for deploying their Internet consumer services, such as Sms+, and Talk+.

The CloudSec checklist has proven useful for Telenor as a cloud customer, to evaluate the security mechanisms and policies of cloud service providers—for example as part of RFQ processes to select service providers.

RELATED DOCUMENTS

- *NIST Cloud Computing Reference Architecture*, NIST Special Publication 500-292, September 2011.
- *Guidelines on Security and Privacy in Public Cloud Computing*, NIST Special Publication 800-144, December 2011.
- *Cloud Controls Matrix (CCM)*, Cloud Security Alliance.
  Available at https://cloudsecurityalliance.org/research/ccm/
- *FedRAMP Security Controls*.
  Available at http://www.fedramp.gov/
- *Procure Secure - A guide to monitoring of security service levels in cloud contracts*, ENISA, April 2012.
- *Opinion 05/2012 on Cloud Computing*, Article 29 Data Protection Working Party, July 2012.

ENDNOTES

[1] Hon, Millard and Walden. *Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now*. Stanford technology law review, Vol. 16, No 1, 2012.

[2] Simon Bradshaw, Christopher Millard, Ian Walden: Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374

[3] *Homomorphic encryption* is a promising technique that allows encrypted data to be processed in the cloud, however due to the computational overhead the technology is still in its infancy.

[4] http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Admin_Access.htm

[5] http://venturebeat.com/2011/09/22/security-lessons-from-the-playstation-network-breach/

[6] Cloud Security Alliance. *Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing*. CSA whitepaper, June 2013.

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[8] Some customers, particularly those from the public sector, also require guarantees that their data is stored within their own country.

[9] Hon, Millard and Walden. *The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing*. International Data Privacy Law, Vol. 1, No. 4, 2011.

[10] http://www.theserverside.com/feature/Are-consumer-cloud-services-or-a-BYOD-mindset-a-bigger-security-threat?utm_medium

[11] http://www.businesscloudnews.com/2013/06/12/moving-services-to-the-cloud-may-reduce-energy-use-up-to-87/

[12] http://www.gartner.com/newsroom/id/2426615

[13] http://www.networkworld.com/news/2012/111412-gartner-cloud-contracts-264270.html