Risk Analysis of TSD - Tjenester for Sensitive Data

Version 4.0
2018-03-08

Espen Grøndahl
IT-Security Officer
UiO

1. Introduction

TSD - Services for Sensitive Data (Tjenester for Sensitive Data in Norwegian) was developed by USIT at the University in the period 2011-2014. It is based on a pilot TSD 1.0 which was made 2008-2011. The system offers a secure environment that meets all legal requirements regarding privacy and protection of sensitive data. The service is meant to host primarily sensitive research data within the health sector, but also other data that require additional protection.

Since it was launched in May 2014 the service is in continuous development to meet the evolving needs of the targeted user communities. This document is the fourth version of the risk assessment and is based on TSD as of February 2018. The previous version of the risk assessment was published in February 2017. This most significant change to the core infrastructure is the addition of the TSD HTTP API for data transport. We have also made changes to administrative procedures which will be noted throughout the text.

2. Background

TSD is in full production from May 2014. This risk assessment is the fourth general assessment of TSD and will be the basis for the regulatory risk which each project manager will have to make before they use the system for storage and processing of sensitive personal data.

3. Limitations

This risk assessment addresses TSD and its major components, as well as surrounding infrastructure that might have direct or indirect impact on the solution. The document does not provide details of the single components, unless it is important to describe the overall risk picture. The technical description of each component is provided in the attached Whitepaper.

This document does not cover the risks associated with special solution implemented to address the needs of single projects, but is based on a general usage patterns. Projects that use the system must supplement with their own judgments which are specific to their projects.

4. Short Description of the solution

A detailed description of the solution can be found in the attached whitepaper and on the service web-pages. Some details cannot be disclosed and are provided only on request.

TSD has physically and logically closed network with strong access control, and operations are performed using automation tools where possible. The infrastructure

consists of virtualized linux and windows environments dedicated to each project, running on a dedicated project VLAN, connected to the central storage facilities. A number of dedicated VLANs are occupied by administrative virtual machines. A cluster of three Active Directory (AD) instances, one physical and two virtual, running on one of the administrative VLANs, is used for user and group administration, and the distribution of host policies. The project machines can only communicate with the resources on their own project VLAN and have no connection with other VLANs or outside networks. Projects do have some openings to the administrative VLANs to enable usage of shared network services and resources. The only network traffic allowed between the administrative machines and the "world" is for the actual user access, logs and license info.

Users access TSD by establishing an encrypted communication to dedicated gateway machines. Login protocols are based on PCoIP (to log on windows machine) or Thinlinc (linux machines). Login requires Two-Factor Authentication using username, password and a one-time code. A person having access to two or more different projects will have a dedicated username per project in order to avoid leakage of data through projects. Functionalities that can enable uncontrolled transfer of data (cut-and-paste functionalities, the mapping of local drives, USB forwarding) are disabled.

All network traffic into and out of TSD is controlled by the firewall. This includes login and data transfer. The latter can be done in one of two ways: 1) using the filelock and/or 2) using the TSD HTTP API.

The Filelock consists of two machines, one physical machine, accessible by the user through a SFTP channel upon two factor-login, and one virtual machine, on the inside of the TSD network that can mount projects areas. The two machines are synchronized, so that a file placed from the outside on the physical machine is automatically copied to the inside and vice versa, in case of export. The Filelock mechanism allows strong control of user import/export privileges and logging of files name and eventually checksum data. The solution is designed to create several barriers towards attack so to minimize the impact of a potential security breach.

The TSD HTTP API also allows data import and export. It supports three authentication methods: basic authentication, TSD two factor authentication and BankID authentication. All API clients are verified by TSD staff and are given access to specific projects on a per-need basis. Basic authentication only allows data import and is only allowed from API clients running on machines with specific IP addresses. The API is integrated with TSD's internal Identity Provider and authentication and authorization system. Two factor authentication using TSD credentials and BankID credentials allow for both data import and export, in principle. The same authorization system applies whereby a project administrator has to grant export rights to a project member. In addition to user authentication, applications have to authenticate themselves towards the API, using a revocable time-limited API key. This allows TSD to revoke access to any application at any time, should it be necessary.

All the users and administrative personnel must log onto the TSD via two factor authentication. Technicians and sys-admins have a user credential so that every operation can be traced and eventually connected to the responsible person.

5. Security requirements

The degree of security is evaluated often along three axes. Confidentiality - ensuring that no one is able to access the data other than those who have legitimate needs. Integrity - ensuring that the data or the code is not manipulated or changed inadvertently. Availability - ensuring that data is available to the right person at the right time.

Data processed in the TSD requires a high degree of confidentiality and integrity. Availability is also important in the sense that the right person shall have access to the right data, but minor focus will be put on ensuring that solutions has an uptime of 24x7. This may change in the future, if it will be decided that the TSD shall host clinical data (e.g. patient data etc). But such a change would require a reconsideration and perhaps significant changes in some components of the infrastructure.

6. Security assessment

6.1 Method

The risk assessment is performed with the methodology used at the University Center for Information Technology (USIT). It follows the guidelines provided by UNINETT and is based on a collection of risk factors that are assessed based on the probability and consequence.

The risk assessment is carried out by evaluating risk elements that can threaten the confidentiality, availability or integrity of TSD. Risk elements are extracted through assessments made in the design and development phase of the solution and finally evaluated in the Council of Changes, a periodic round table with decisional power involving the technical advisors, the administrative leaders and the IT-security officer.

The present risk assessment methodology is an updated version of the previous one and it is aligned with UNINETT guidelines for risk assessments. Compared to the previous risk analysis conducted in 2017, the only significant infrastructural change has been the addition of the HTTP API. This has been factored into the risk analysis.

6.2 Members

The assessment is done by:

Espen Grøndahl – IT-Security officer
Gard Thomassen – Service owner
Leon du Toit – Service manager
Morten Werner Forsbing – Technical Coordinator

7. Acceptance Criteria

Security will always be a consideration and a balance between usability and security. The level of usability should be high enough that the possibility to choose a less secure alternative is not wishful. Some risks will therefore be acceptable to get the functionality that users need.

However given the high security profile of the solution very few risks are considered acceptable. There must be low risk associated with inadvertently exposure of sensitive data. If there are security breaches, confidentiality and integrity are prioritized over availability. This will be emphasized in the risk assessment.

7.1 Evaluation Scales

Risk elements are evaluated on a scale from 1-4, probability, and 1-4 in consequence, where 1 is associated with low probability, or little or no consequence and 4 is very likely and very severe consequence.

In detail, this security assessment adopts the scale suggested by UNINETT to evaluate the probability:

Low (1)	**Medium (2)**	**High (3)**	**Very High (4)**
One time every 10 years or more seldom	One time per year or more seldom	One time per month or more seldom	Weekly

In details, this security assessment adopts the following scale to evaluate the consequences:

	Personal Data	**Project Owner**	**Service Provider (USIT)**
Very Severe Consequences (4)	Incident involving unjustifiable lack of security for personal data	- Incident involving loss of data or communication of data to unauthorized parties - Incident leading to irreparable financial losses	
Severe Consequence (3)		- Incident involving loss of data - Incident leading to significant financial losses	Incident leading to substantial and irreparable financial loss or serious loss of reputation / integrity.
Moderate Consequences (2)		Incident involving service with inadequate quality and low availability	Incident leading to substantial financial loss that can be recovered or loss of reputation / integrity due to

			compromising of infringing information
Little or no Consequences (4)			incident involving loss of trust between the project owner and service provider

Each risk element is associated with a value obtained by multiplying the values associated with the probability and the consequences.

7.2 Risk elements between 1 and 3:

Risk elements between 1 and 4 are considered acceptable either as they are or after the implementation of dedicated measures and/or routines.

7.3 Risk elements between 4 and 8:

Risk elements between 5 and 8 must be evaluated carefully. They might be considered as acceptable for a short period of time, while the necessary mitigating safeguards are being planned.

7.4 Risk elements between 9 and 16:

Risk elements between 9 and 16 are not acceptable. These risks require service interruption and/or must be compensated with manual control and strong routines until the risk is reduced.

8. Description and assessment of the risk elements

Risk elements are listed in the attached excel file. They are numbered with serial number. Here is a description and assessment of elements requiring mitigating measures or special attention (category [4-8]).

Risk element 5

The risk for data leakage between projects as a consequence of intentional action has inevitably high consequences but low probability. The projects have a dedicated VLAN and no network traffic between project VLANs is allowed. In addition, the access to the resources on a given project is given through group policies. The implemented safeguards have been tested in a penetration test undergone by TSD in summer 2016 and conducted by a well-known security expert. The test was successfully passed as the attacker did not manage to leak data between projects.

Risk element 7

The risk has high consequence but low probability. The logon to the TSD is behind two factor authentication and therefore requires valid username password and one-time code. In the rare case in which the username and password are guessed, the one-time code is impossible to guess.

Risk element 14

The risk that data are exported through mechanism other than the filelock is continuously evaluated by periodic penetrating testing and adequate safeguards are implemented as different scenarios are discovered.

Risk element 15

The risk of someone hacking the TSD API, thereby gaining access to data stored in memory, as it is being transferred over the network. This is mitigated by two factors: 1) unless in the project area, or in an administrative VLAN protected by the firewall, no data is kept in memory unless encrypted, and 2) the API architecture is such that the application server which has access to plain-text data, stored in the project, is protected by several layers and authentication mechanisms with high level of assurance.

Risk element 16

The risk of damages caused by disloyal sys-admins and technical staff members is reduced by increasing the awareness of the technicians with regards to the importance of the service and the consequences of its failure. In addition, every sys-admin uses private dedicated user credentials in TSD and most of the operations are traceable.

Risk element 19

The event of fire or similar unfortunate events might have severe consequences. Even if the backups of the disks are kept in a different physical location, the disruption of the machine room could result into severe damage of the service infrastructure and long outage. Existing safeguards consist of fire alarms and monitoring of the machine room. In addition, TSD is investigating a mechanism to make off-site replicas of the data repository and infrastructure.

Risk element 20

The service is located in a room behind three sets of doors, the first (more extern) requires a valid card to enter, while the second and third requires card and code. Both the card and the code are private to the technicians and are issued by the University of Oslo. The system is not locally controlled, but centrally controlled at UiO. To reduce the risk even further inadvertently TSD are working to implement an extra lock to secure the second innermost door. The entire area including machine-rooms are under video surveillance once entering the first door. However, the combined use of the code and the card significantly reduces the probability of a successful unauthorized access. The risk element, compared to the previous risk assessment has been downgraded to acceptable risk (was 6).

9. Final assessment and follow up

Every point on the previous version of the risk assessment has been rectified in such a way that the risk has been reduced to an acceptable level.

10. Conclusion

According to our assessment, the most serious risk elements has been downgraded to acceptable risks. The solution has been designed from the start to have very high security standards and the present assessment has revealed no weaknesses or backdoors into the system.

TSD has also established a system for incident handling. Cases are reported and archived so that we can easily look at trends and prevent future similar problems. Serious discrepancies will be reported to the end users.

A Council of Changes (in Norwegian “Endringsråd”) has been established to periodically evaluate the security aspects of the present set up and of on-going developments. The Council involves the IT-security officer, the service owner, the service manager, the technical coordinator and the security experts. Main customer representatives are invited, but veto lies with the IT-security officer. The Council supervises any system-changes and guarantee that the security standards are respected even when the changes are so small that they do not invoke a Risk Assessment upgrade.

11. Attachments

A. ”Whitepaper TSD ”
B. Risk elements TSD