Security whitepaper

Pathology Image Exchange

palga

Platform voor het delen van digitale pathologiebeelden

DOC-PJOS-ALTJW2 V.2.1

Pathology Image Exchange

Security Whitepaper

This whitepaper describes the security aspects of the Pathology Image Exchange (PIE). PIE is designed to be a “Patient Privacy First” solution: protection of patient privacy and hospital security have been the primary drivers of the total PIE architecture. In this whitepaper we describe how both are achieved.

Patient Privacy

PIE deals with two types of information: Patient Identifying Data and Images, which are separated at the source: the Laboratory Information System (LIS). These information streams are joined in the receiving laboratory again using a random one-time key.

Patient Identifying Data via Lab2Lab

For many use cases the use of Patient Data is medically required, for example to retrieve a medical history for the patient allowing a higher quality diagnosis. Transferring identifying information, like name, date of birth and BSN are required by law to prevent patient mix-ups.

In order to transport this data between two laboratories, the PALGA Lab2Lab solution is used. This communication channel is a proven solution, already used for order communication between the Dutch pathology departments, allowing secure communication at several levels. It provides the following:

- End-to-End message encryption (from Laboratory to Laboratory), with mutual authentication.
- Mutually authenticated SSL-based transport encryption between all servers.
- Dedicated communication channels (e.g. VPN or dedicated KPN connection). Site-to-Site communication based on hospital requirements.

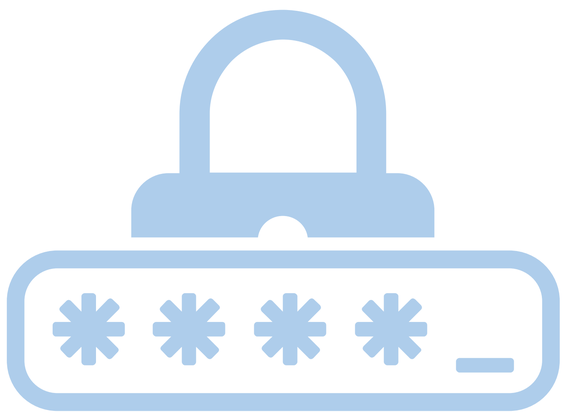
These three layers of security are independently implemented and are based on their own independent PKI-certificate authorities, making eavesdropping on this communication impossible.

Data is stored encrypted, at a secure location: RAM Infotechnology

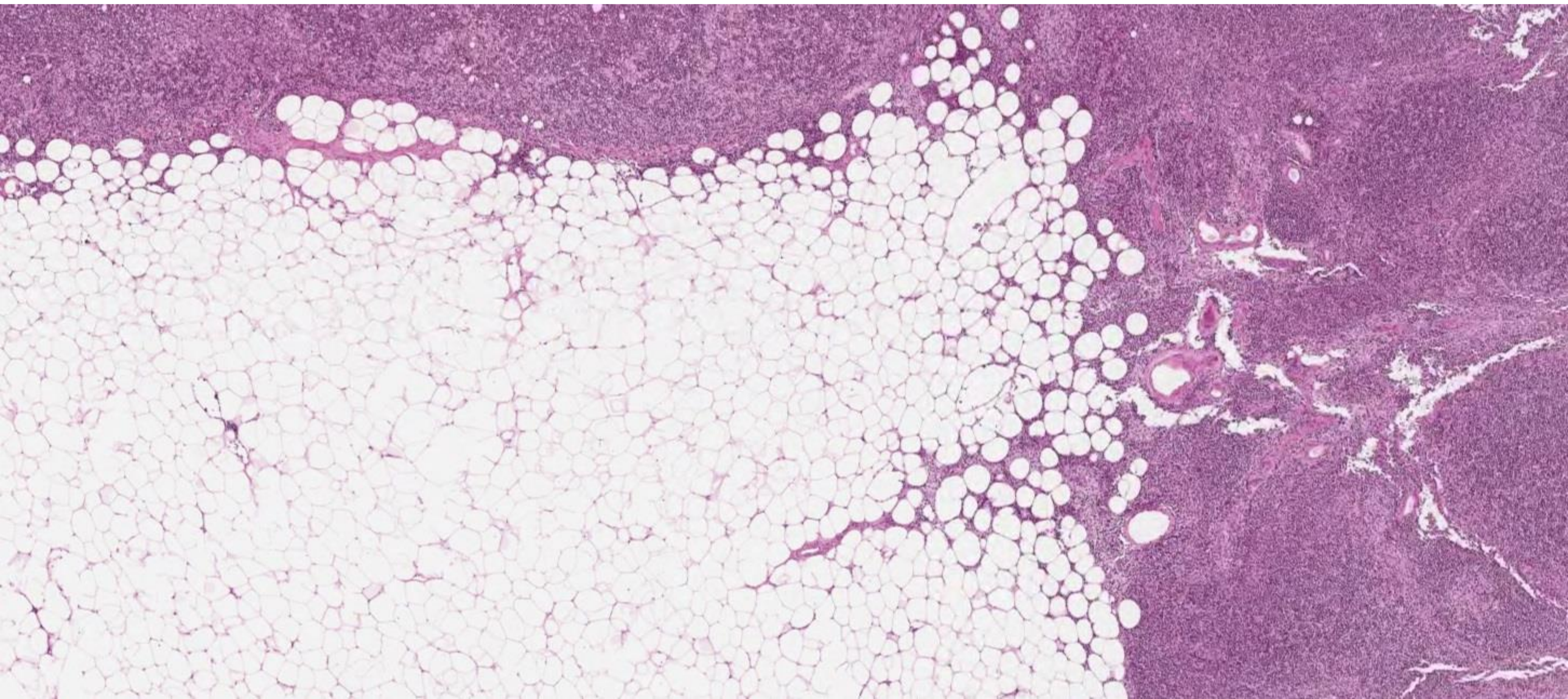
Images via PIE

The images are anonymized: they are anonymous pixels that can only be related to a patient by using the random one-time key (case key) that is transferred along with the order through the secure Lab2Lab channel. Even the meta-data of a pathology image is scrubbed from identifying data. Only meta-data transferred along with the image are the sex, age and clinical question of the patient.

Despite the low impact on patient privacy, the PIE solution is well-protected. It provides:



- Central 2-factor-authentication for all pathologists and an extensive rights system shielding images from unauthorized use.
- Central PKI Encrypted Launch string of the PIE Application.
- Mutually authenticated SSL-based transport encryption.
- PIE application traffic will be actively monitored for malicious content.



In line with the PIE requirements cases held in PIE are anonymised. This will be achieved through the following mechanisms depending on how the case is sent into PIE.

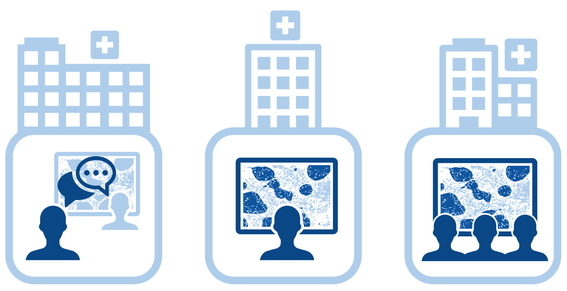
Where the automated (locally installed) uploader is used, the images will be cleaned using the uploader component before sending it to the central PIE server if that was not done by the system providing the images to the uploader component.

When the manual upload mechanism is used, the person uploading the images is responsible for anonymizing the images.

When the platform receives the images at the central PIE server, all incoming images will be cleaned (again) to prevent any technical/human mistake that could compromise the anonymity of the PIE solution.

Hospital Security

To protect Hospital/Laboratory security, several guiding principles have been used:



- The PIE and Lab2Lab solutions will always require communication to be initiated by the hospital.
- Communication is always performed over dedicated (trusted) lines, set up according to hospital security policy.
- The PIE solution will not require open incoming ports in the hospital firewall.

This way, the PIE and Lab2Lab solutions are easily to secure from an hospital perspective.

Service Security

RAM Infotechnology, the hosting provider is specialized in storage of medical data. The following specific security measures are in place to protect the PIE solution.

The Internet connection is segregated from the secure stores via a DMZ, ensuring that only the appropriate services can access the secure data.

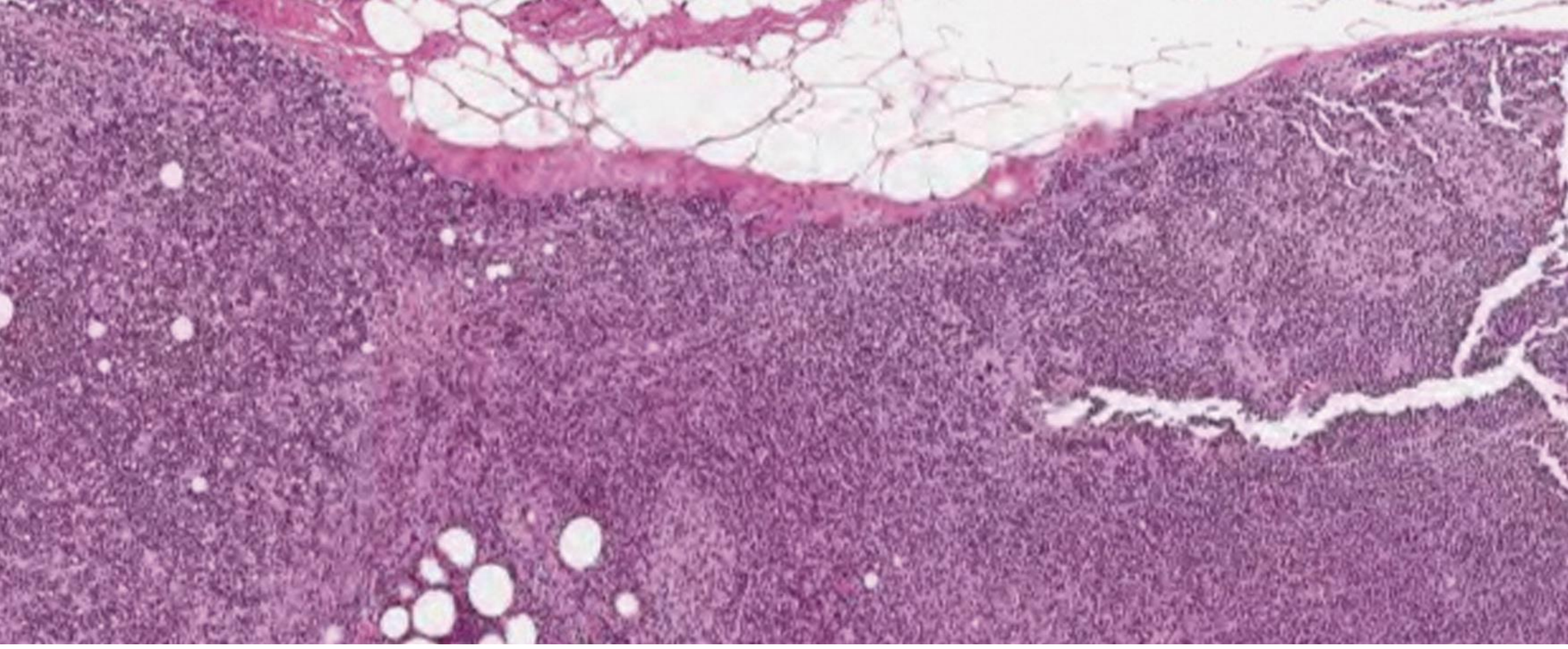
All connections are secured using an SHA256 SSL certificate.

VM Based Server design, including back-up.

Certification against the ISO27001/NEN7510 standard, including:

- Active automated patch management.
- Intrusion detection schemes active in the network.
- Active Virus Scanning.
- Server hardening.
- Monitoring and logging.

Regular audits by Stichting PALGA and external certification bodies.



Pathology Image Exchange

palga

Het platform voor het delen van digitale Pathologie beelden wordt mede mogelijk gemaakt door:

NEDERLANDSE VERENIGING VOOR PATHOLOGIE

Stichting Pathologie Projecten

iKNL integraal kankercentrum Nederland

SECTRA
Knowledge and passion

T HEALTHCARE SOLUTIONS
ram infotechnology