Infosheet
sett – BioMedIT's Secure Encryption and Transfer Tool

Background – why was sett created?

Transfer of sensitive personal data from a Data Provider into the BioMedIT network requires data to be encrypted and sent using secure methods. Not all users are comfortable with command line tools to encrypt, sign and transfer data. In early 2019 the BioMedIT Interoperability Working Group (BIWG) started to develop **sett**, a tool for secure data transfer with both a graphical user interface (GUI) and a command line interface (CLI). With the release of version 1.0 the tool is now available for public use.

Why should I use this tool?

In the context of BioMedIT **sett** streamlines the tedious process of data packaging, encryption, signing and transfer. It is available in both a GUI and a CLI version. Data Providers can use it for PGP key generation, key management and data packaging, encryption, and transfer. Data Managers of a research project can use it for key generation and management, and decryption and unpacking of the received data.

What is the tool based on?

The tool uses GnuPG v2 for signature, encryption and. decryption, and Python3 as a codebase to accomplish its tasks. The ownership and owner identity of all public PGP keys used within is first verified and only then signed by the SPHN Data Coordination Centre (DCC). Private keys remain with their owner and are never disclosed. Transfers of data packages are carried out on trusted networks using either SFTP or Liquid Files.

What is needed for a data transfer other than sett?

Data Providers who need to send data must have:

- a valid Data Transfer Request from a Data Recipient via DCC
- their public key signed by DCC
- destination information if one of the predefined destinations in **sett** is not used

Can I modify sett or use it for projects not related to BioMedIT?

Yes. The tool is open source and licensed under the LGPL. By unchecking the *Validate Project ID* option in **sett** other project identifiers may be used. Data packages can be sent to any security compliant endpoint.

What if I do not want to use sett for data encryption and transfer of data in BioMedIT?

sett was designed as a helper tool and is the recommended solution for secure data transfer. To ensure a Data Recipient can decrypt the data package using **sett**, the data package to be sent must comply with the **sett** specification for encryption, signature and structure.

Where can I find more information?

Contact BioMedIT at dcc@sib.swiss, a member of the BIWG, or go to https://gitlab.com/biomedit/sett where user documentation, codebase and data packaging specification can be accessed.

Problems with sett?

Send an email to biomedit@sib.swiss to open a ticket with your problem.

A project of SAMW ASSM
Schweizerische Akademie der Medizinischen Wissenschaften
Académie Suisse des Sciences Médicales
Accademia Svizzera delle Scienze Mediche
Swiss Academy of Medical Sciences

SIB Swiss Institute of Bioinformatics

Swiss Institute of Bioinformatics (SIB)
Personalized Health Informatics Group (PHI)
Elisabethenstrasse 43
CH-4063 Basel, Switzerland

The Personalized Health Informatics Group manages
the SPHN Data Coordination Centre and the BioMedIT project