

# Explaining Bug 18908

Nils Gähler  
Bug Squashing Seminar

**dkfz.**

GERMAN  
CANCER RESEARCH CENTER  
IN THE HELMHOLTZ ASSOCIATION



50 Years – Research for  
A Life Without Cancer

Welcome  
to the DKFZ!

dkfz.

dkfz.

GERMAN  
CANCER RESEARCH CENTER  
IN THE HELMHOLTZ ASSOCIATION



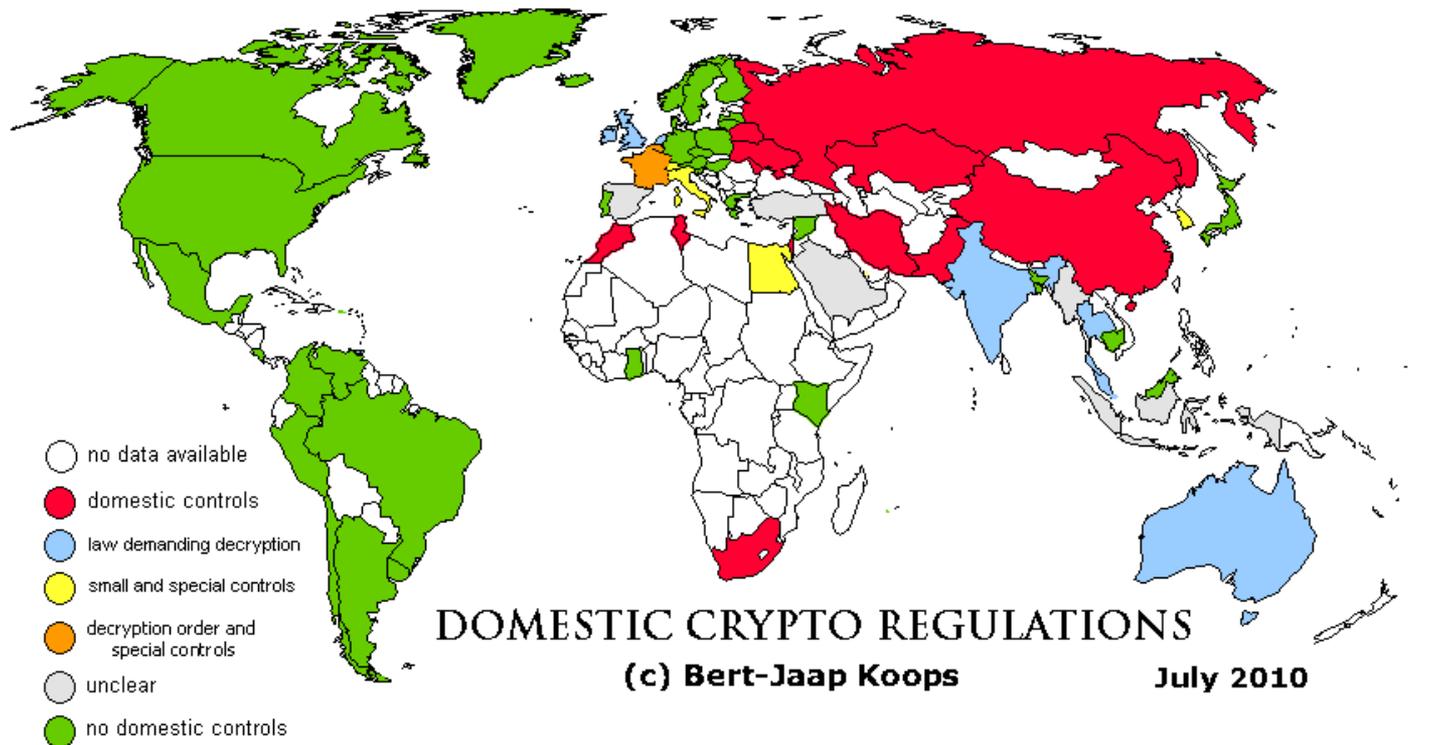
50 Years – Research for  
A Life Without Cancer

## Ehh... What is Bug 18908?

- Title:  
SSL Problems with XNAT Plugin connecting to HTTPS server address
- A. Fetzer:  
This is a known issue for Qt:  
<http://stackoverflow.com/questions/20351155/how-can-i-enable-ssl-in-qt-windows-application>
- S. Kislinskiy:  
This is a deliberate decision of the Qt team due to import/export restrictions regarding OpenSSL to some parts of the world

# But we're not in North Korea!

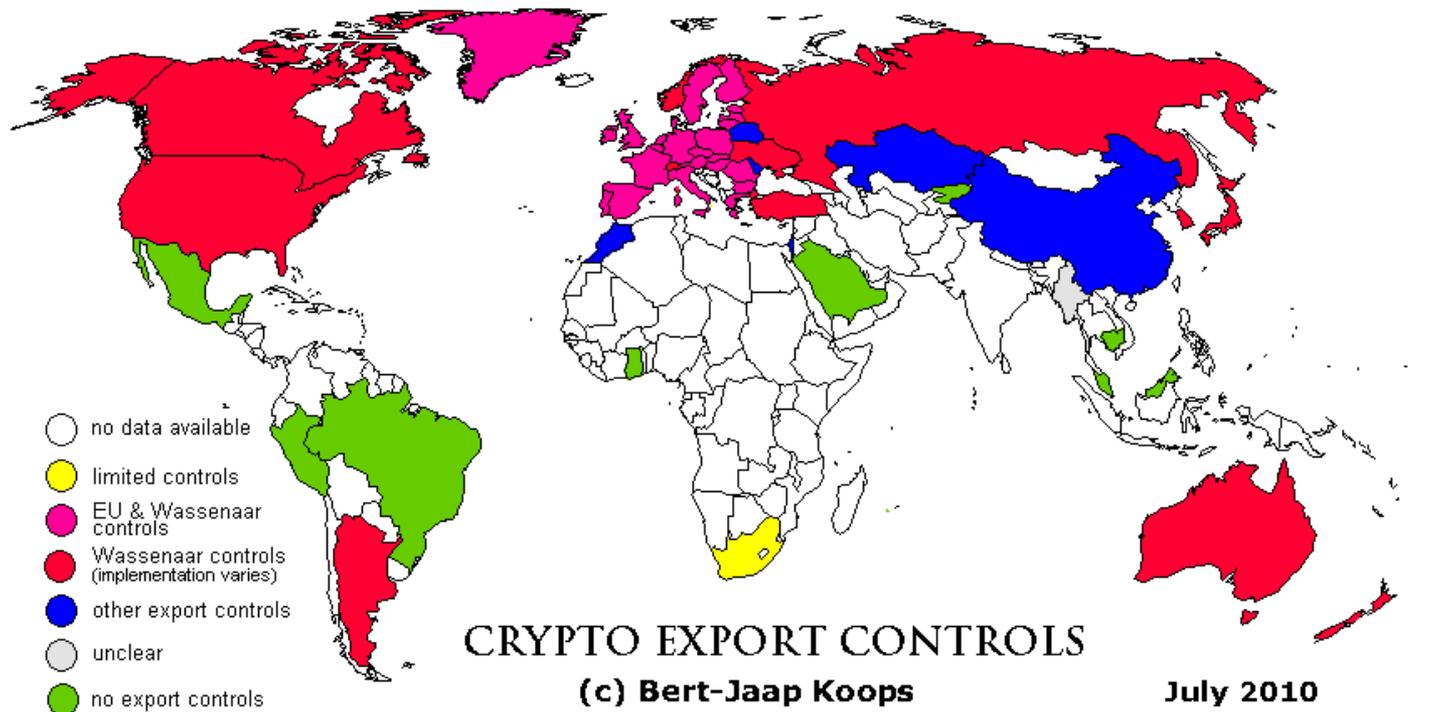
- Cryptography (nearly) completely forbidden in Cuba, Iran, North Korea, Sudan, Syria



[cryptolaw.org]

# We're in Germany! So everything is fine.

- Really?



[cryptolaw.org]

# Wassenaar-Arrangement (since 1996)

**THE WASSENAAR ARRANGEMENT**  
On Export Controls for Conventional Arms and Dual-Use Goods and Technologies

HOME | ABOUT US | PARTICIPATING STATES | **CONTRIBUTING COUNTRIES** | BEST PRACTICES | **ANNOUNCEMENTS** | OUTREACH | RELATED LINKS

**About Us**

The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. The aim is also to prevent the acquisition of these items by terrorists.

Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

**What's New**

- List of Dual-Use Goods and Technologies and Munitions List as at Apr. 2016
- Statement by the 2015 Plenary Chair, 3 Dec 2015
- Best Practice Guidelines for Transit or Transshipment
- Elements for the Effective Fulfilment of National Reporting Requirements
- Summary of Changes to the Lists as at Dec. 2015
- WA 20th Anniversary 2016

**Search**

wassenaar.org

Search ....

**Contact**

Wassenaar Arrangement Secretariat  
Vienna, Austria

CONTACT US

READ MORE

Participating States:

Wassenaar: 5. A. 2. a. 1.

- a. A "symmetric algorithm" employing a key length in excess of **56 bits**;
- b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:
  - 1. Factorisation of integers in excess of **512 bits (e.g., RSA)**;
  - 2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over  $Z/pZ$ ); or
  - 3. Discrete logarithms in a group other than mentioned in 5. A. 2. a. 1. b. 2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);

[<http://www.wassenaar.org/wp-content/uploads/2016/04/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf>]

## Are we screwed?

NO!

- The Lists [WA] do not control "software" which is any of the following:
  - 1. (...)
  - 2. "In the public domain"; or
  - 3. (...)

Public Domain?

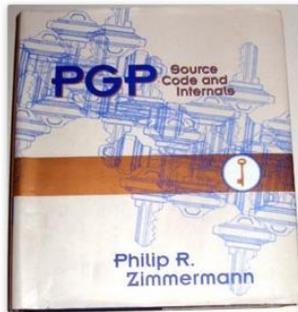
- This means "technology" or "software" which has been made available without restrictions upon its further dissemination.  
*Note: Copyright restrictions do not remove "technology" or "software" from being "in the public domain".*

[<http://www.wassenaar.org/wp-content/uploads/2016/04/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf>]

## Take-Home-Messages

- OpenSSL in Germany is fine.
- OpenSSL connections to other countries participating in the WA is fine.
- OpenSSL connections to other countries **not** participating in the WA is fine for you, for the other maybe not: ⚡
- Implementing cryptographic algorithms that are **not** in public domain: ⚡
- Developing algorithms with copyright and publish them in the public domain is fine.
- Bringing your MITK-Installation with XNAT to Syria, North Korea: ⚡

- Before WA: Strong restrictions e.g. in USA
- Source code of PGP was printed as a book in 1995 and sold worldwide and transcribed manually by 60 volunteers.
- Export of books is protected by the First Amendment.
- PGP available all over the world. 😊



See all 2 images

### PGP: Source Code and Internals Hardcover – June 9, 1995

by Philip R. Zimmermann (Author)

★★★★★ 1 customer review

See all 2 formats and editions

Hardcover  
from \$174.99

12 Used from \$174.99  
2 New from \$433.80

**Prime**student **FREE TWO-DAY SHIPPING**  
FOR COLLEGE STUDENTS [Learn more](#)

PGP (Pretty Good Privacy) is a computer program for the encryption of data and electronic mail, a powerful "envelope" that allows individuals the same privacy in their communications as enjoyed by governments and large corporations. PGP, which is freely available on the internet, uses public-key cryptography - specifically the RSA algorithm, which is particularly well-suited to the needs of computer-mediated communications. This book contains a formatted version of the complete source code for the latest release (2.6.2) of PGP.

Thank you for  
your attention!

Further  
information  
on [www.dkfz.de](http://www.dkfz.de)

**dkfz.**

GERMAN  
CANCER RESEARCH CENTER  
IN THE HELMHOLTZ ASSOCIATION

50 Years – Research for  
A Life Without Cancer