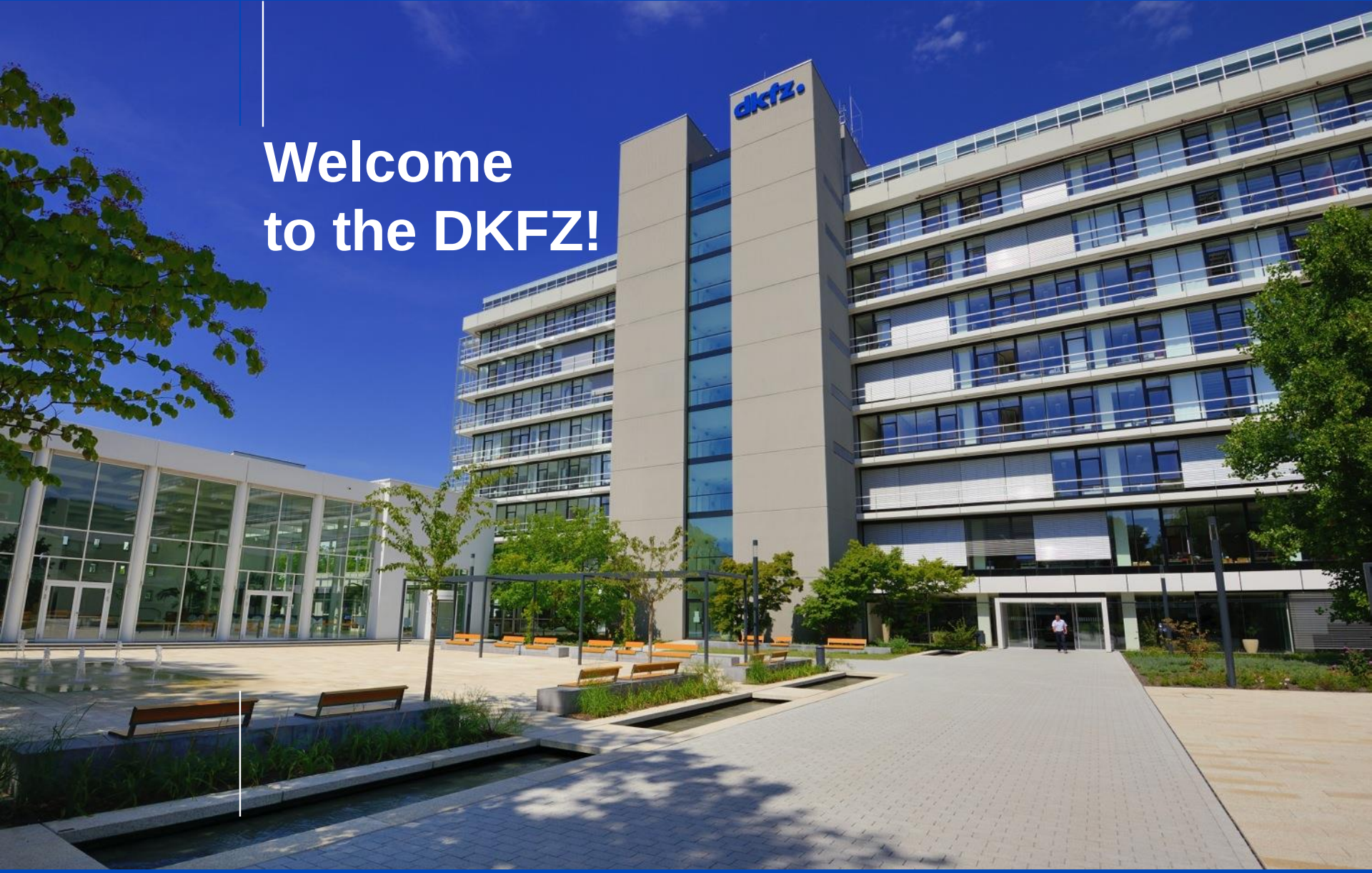
Explaining Bug 18908

Nils Gählert

Bug Squashing Seminar



Welcome to the DKFZ!

dkfz.
GERMAN CANCER RESEARCH CENTER
IN THE HELMHOLTZ ASSOCIATION

50 Years – Research for
A Life Without Cancer

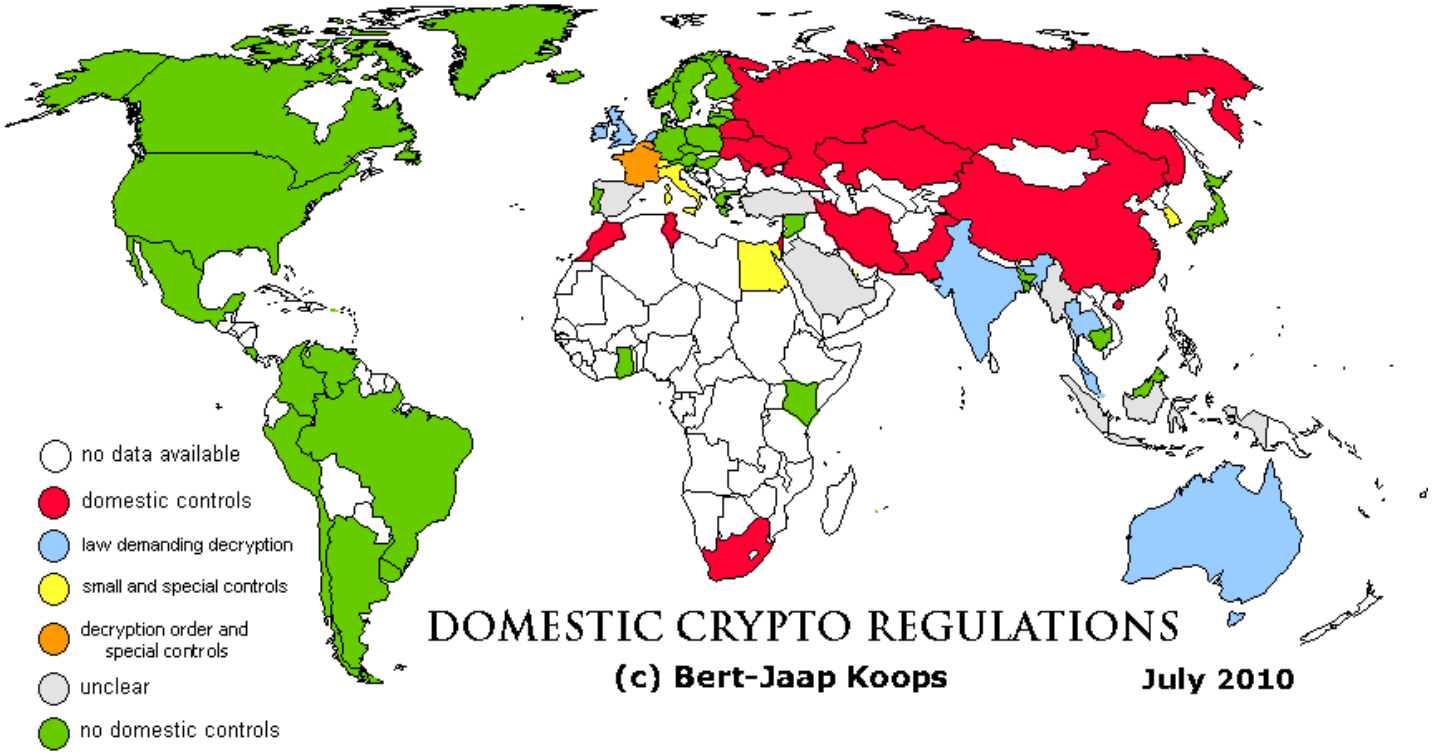
Ehh… What is Bug 18908?

dkfz.
50 Years – Research for
A Life Without Cancer

- Title:
  SSL Problems with XNAT Plugin connecting to HTTPS server address
- A. Fetzer:
  This is a know 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!

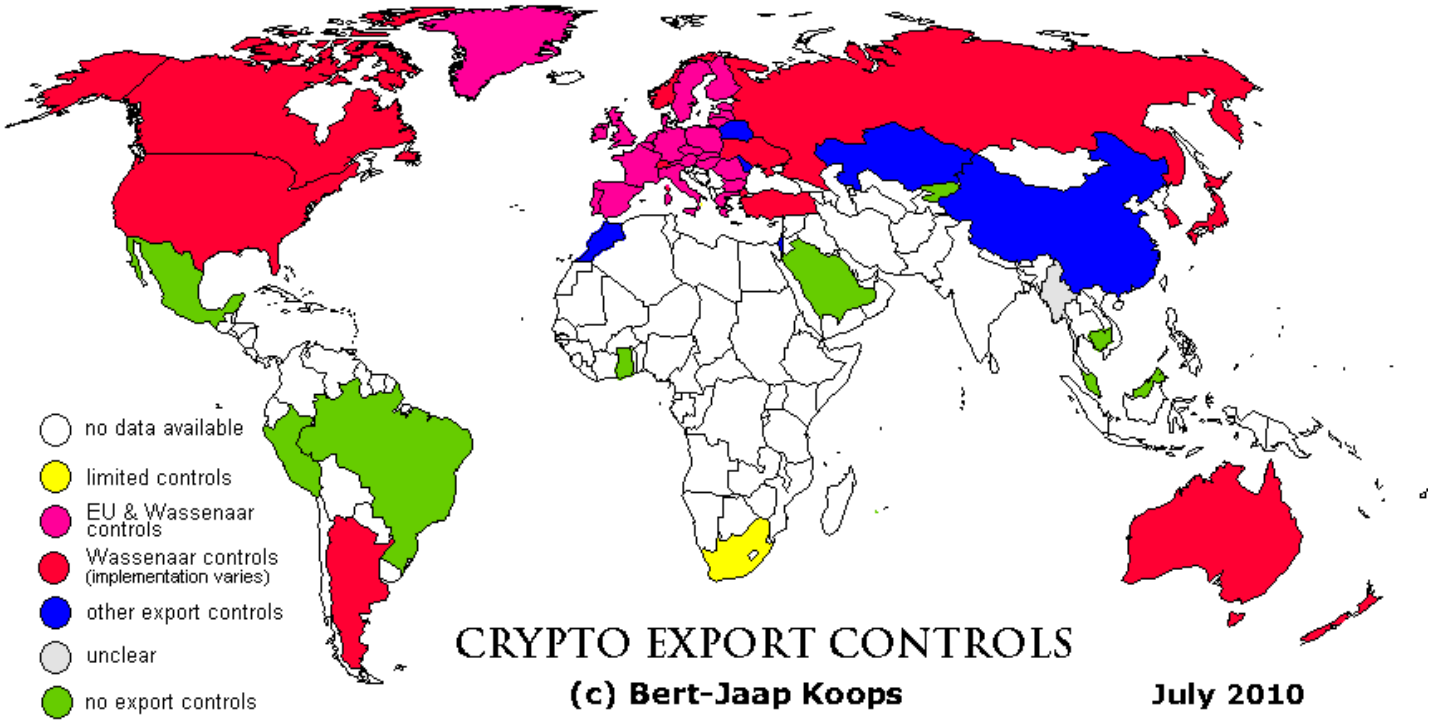
- Cryptography (nearly) completely forbidden in Cuba, Iran, North Korea, Sudan, Syria



[cryptolaw.org]

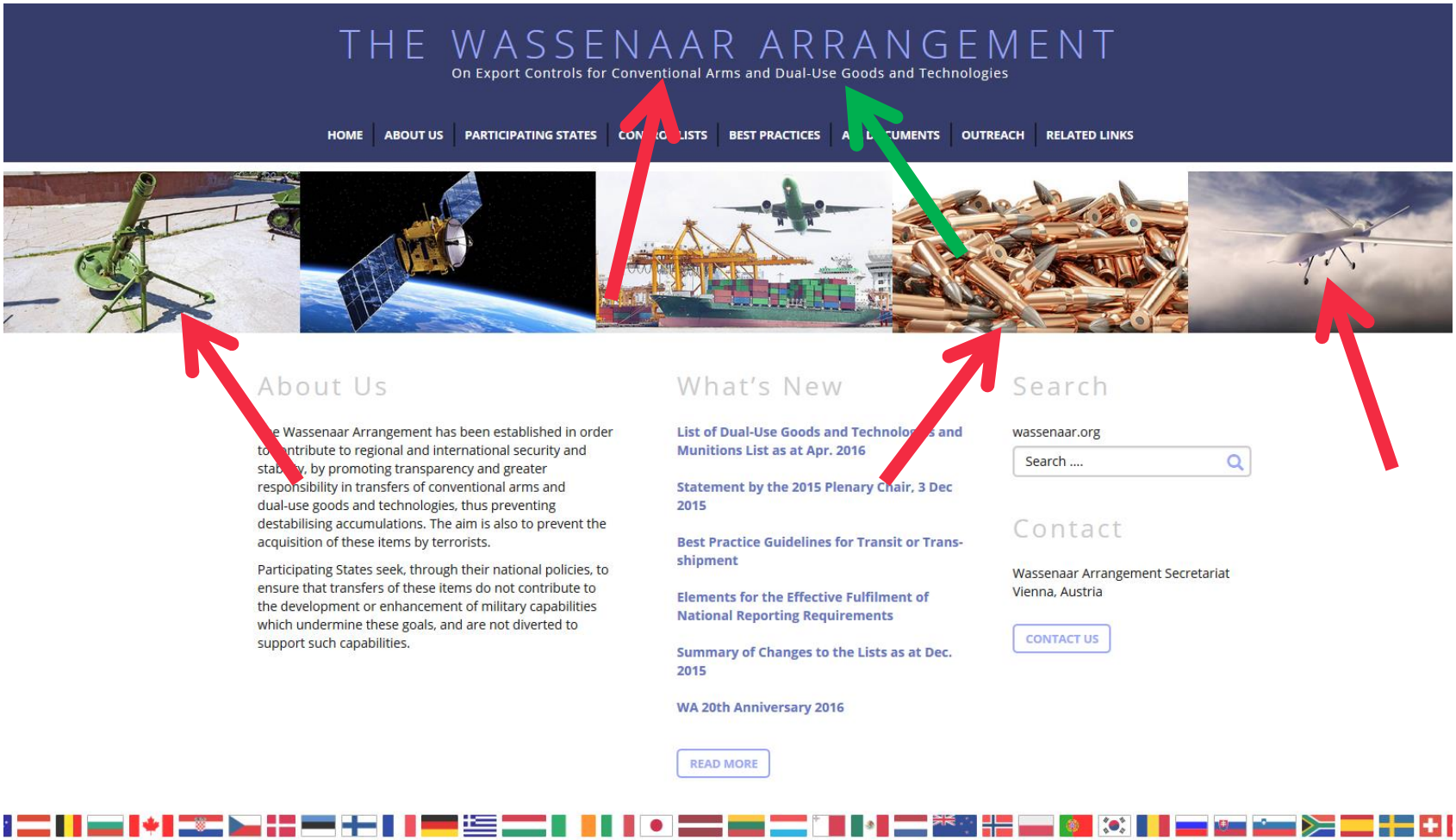
We‘re in Germany! So everything is fine.

- Really?



[cryptolaw.org]

Wassenaar-Arrangement (since 1996)



Cryptography as Dual-Use-Good

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".*

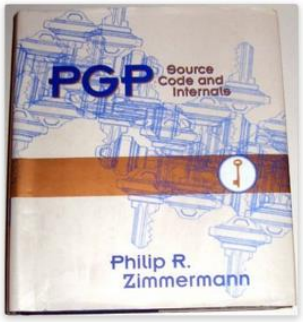
[http://www.wassenaar.org/wp-content/uploads/2016/04/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf]

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: ↯

Fun Fact

- 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

Primestudent 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 vesion 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

dkfz. GERMAN CANCER RESEARCH CENTER IN THE HELMHOLTZ ASSOCIATION

50 Years – Research for A Life Without Cancer