

OpenPKSD

<http://openpkd.org>

Hironobu SUZUKI

<hironobu@h2np.net>

OpenPGP BOF @ CRYPTO2003

Hironobu's Version of PKSD

- Started in 2001/Apr
 - As Free Software
 - Got 2 years budget from IPA, governmental organization (<http://www.ipa.go.jp>)
 - About \$200,000USD to OpenPKSD.ORG project
 - Hironobu, Iwate Prefecture University and Osaka City University

Goal

- Good performance keyserver
 - To use like as Horowitz's pksd
 - SQL database back-end system
 - Cluster extension
- Expandable and flexible program structure
- Easy system management
- (Academic) documents for Japanese community

About OpenPKSD (1)

- HKP
 - Support: get, index, search by 32/64 bit Key ID and mail address in User ID
 - Not Support: vindex, fingerprint, search by “free term”
- HKP via port 80
 - Access via PGP/GPG across F/W
 - Access via Web browser

About OpenPKSD (2)

- Mail sync
 - It can work with Horowitz's PKSD
- Ihave/Sendme
 - This is a tool for key synchronization and can use with Horowitz's keyserver
 - It will be included in next release

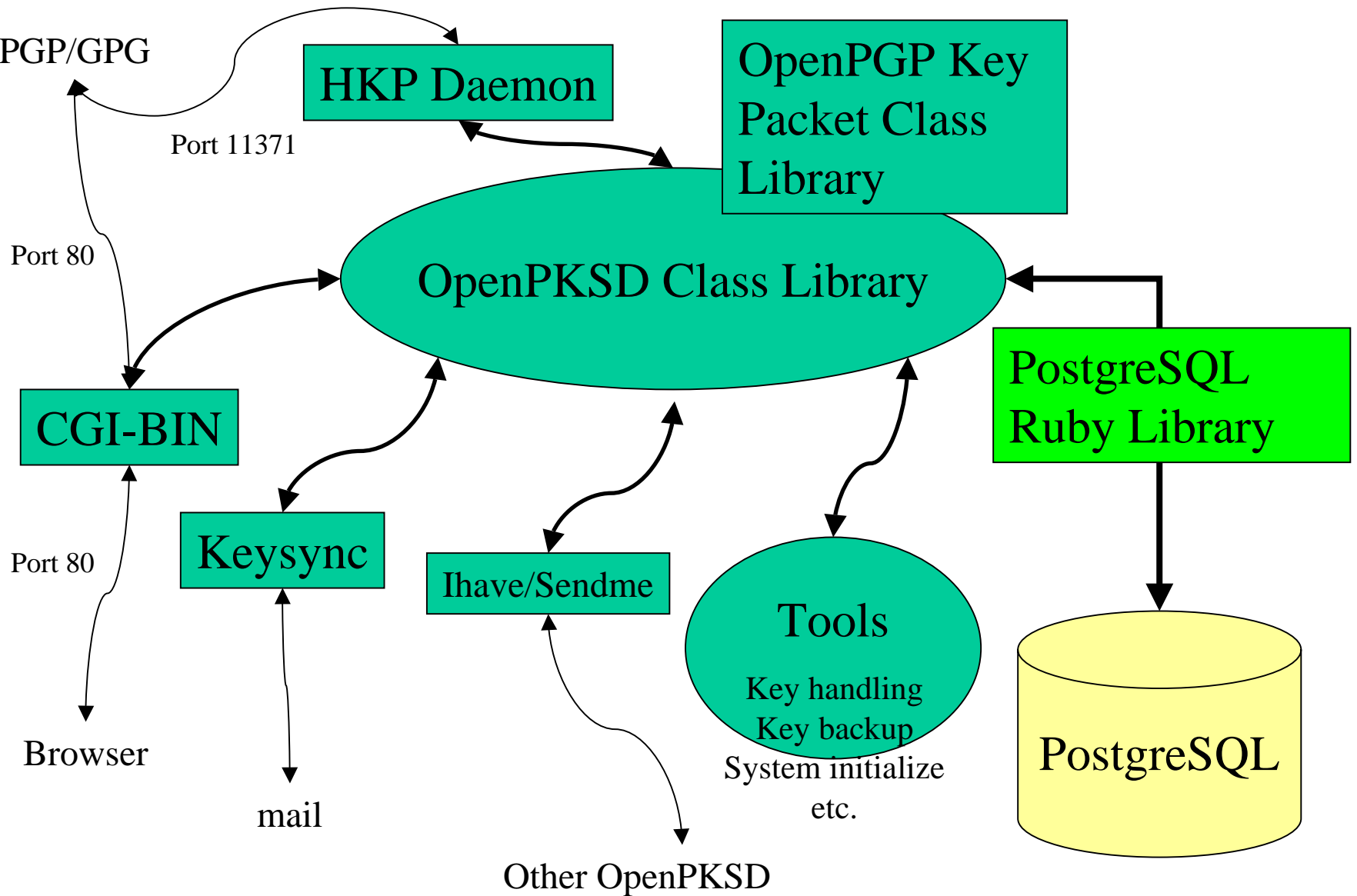
About OpenPKSD (3)

- SQL database back-end
 - Technically, SQL92 format
 - PostgreSQL (current)
 - MySQL, ORACLE, DB/2 and other SQL database (not supported yet)
 - Implementation is easy (maybe) because it would be done for making subclass of OpenPKSD_SQL

About OpenPKSD (4)

- Access control supported
 - Data flow control to avoid heavy load
 - Very simple algorithm and it should be more intelligent
 - Allow/deny accessing by IP addresses
 - “hook” is available but not implement yet
- Programming language RUBY
 - So-called light-weight programming language
 - No bufferflow ☺
 - Easy to expand
 - OpenPKSD design is based on Object-Oriented and build on OpenPGP and OpenPKSD classes

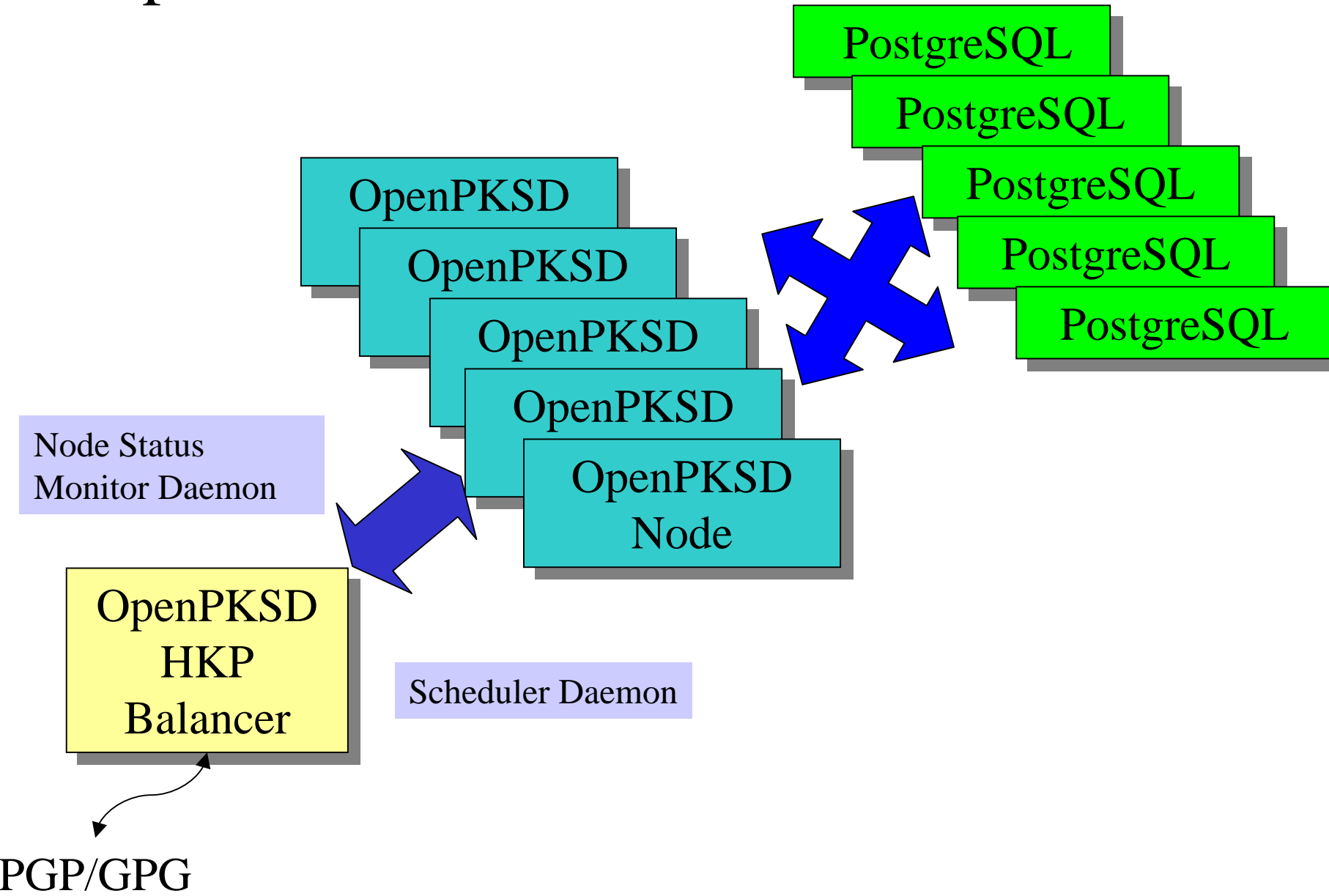
OpenPKSD Program Structure



Cluster Version of OpenPKSD

- Experimental development (in 2002)
- HKP balancer and key processing nodes
 - It works well and it will be distributed as OpenPKSD extension package
- PostgreSQL Cluster
 - It works but inefficient
 - Forget it!!

OpenPKSD Cluster Structure



Known BUG

- Key merge bug
 - My key check algorithm is fragile and some time failure
 - It is hard to find “error case” in huge keyring
 - No more ad-hoc debugging
 - I will change it to robust algorithm

What Next? – Further Works

- OpenPKSD group server
 - Pure RUBY system (No SQL database) and easy to install and management
- Trust key update
 - Update only by signed export public key file
 - More performance are required and cluster OpenPKSD is our answer

All materials are available from

<http://openpksd.org>