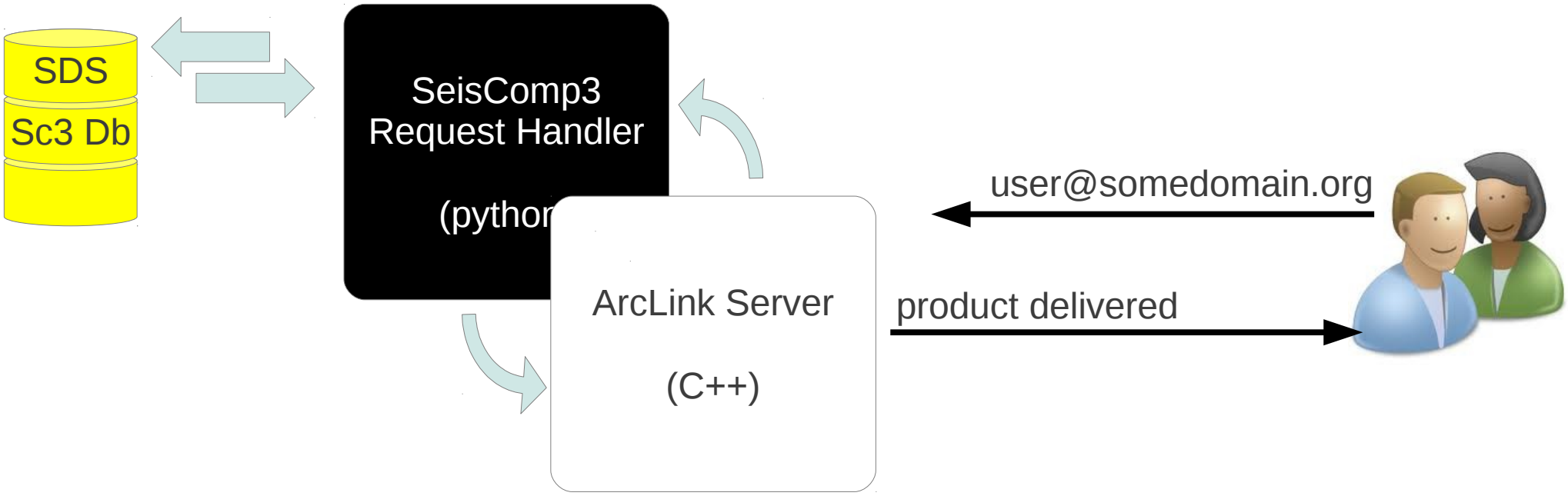
New Features (encryption)

Marcelo Bianchi & Andres Heinloo

22nd September 2011

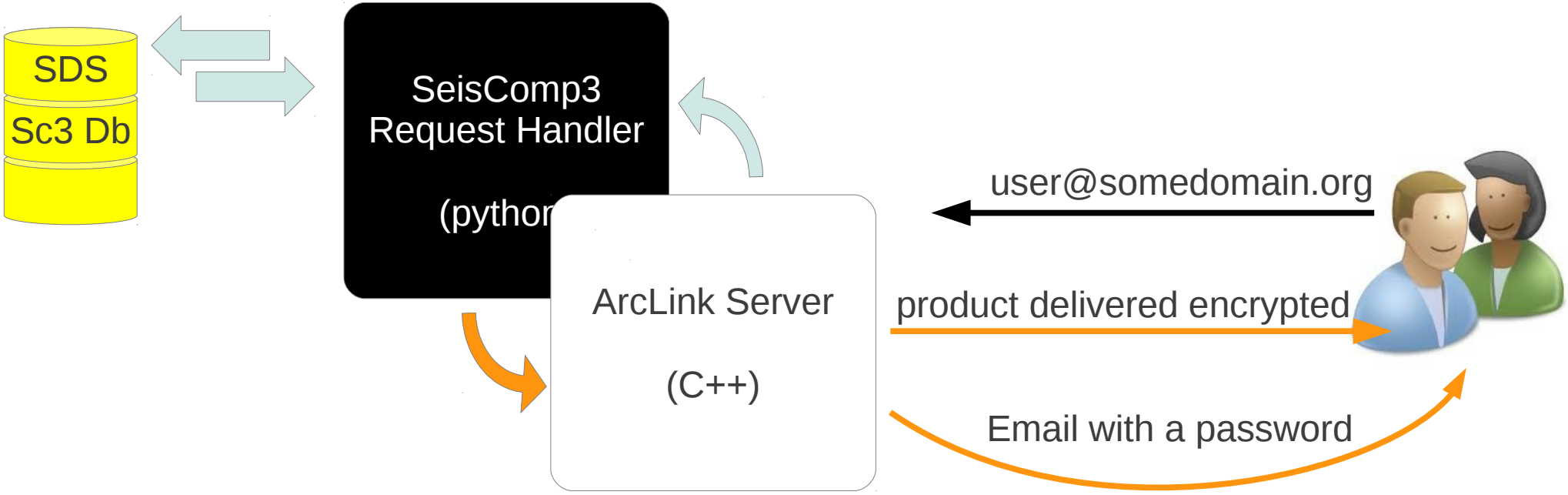
ArcLink Authentication

- On an ArcLink connection the user normally gives his/her email (as identifier) and ArcLink trust this. The request handler check this email against the station/network requested and, if the email is authorized, the product is prepared & delivered.



Encryption

- The encryption is implemented to complement the authentication schema. Nothing will change until the authorization, but after that, the product will be delivered encrypted if the network/station is restricted.



How the encryption is done

- The encryption is done using the openSSL library during the delivery of the request.
  - This allows multiples volumes from the same request to be merged before delivering.
- The algorithm chosen was DES-CBC (same as IRIS uses). The password is just a string that is used to derive the encryption Key & Salt.
- The encrypted files should be decompressed by the openssl tool (from openSSL package) or any other compatible tool.

Password file

This is the password file generated by ArcLink server. Each time a new user receives a password this file is updated. The passwords are stored encrypted with the ArcLink admin password.

```
~/seiscomp3/arclink/status# cat password.txt
mbianchi@gfz-potsdam.de:cd98a64cb17deeaa9124b8e70e5b9027
pevans@gfz-potsdam.de:ed946bed7cd58c76d2e9f5178817320f
m.tchelo@gmail.com:712310b6d8f113f82720340ff56bfe5e
mail@robert-barsch.de:4ba32e0444b43a20f2e253bdca48ce5a
test@obspy.org:1d4fc6144cf167d7e4159383b8744bd6
```

If you remove a line from this file, it is enough to reset the user password to a new one. Also, changing the ArcLink password would make this file unreadable.

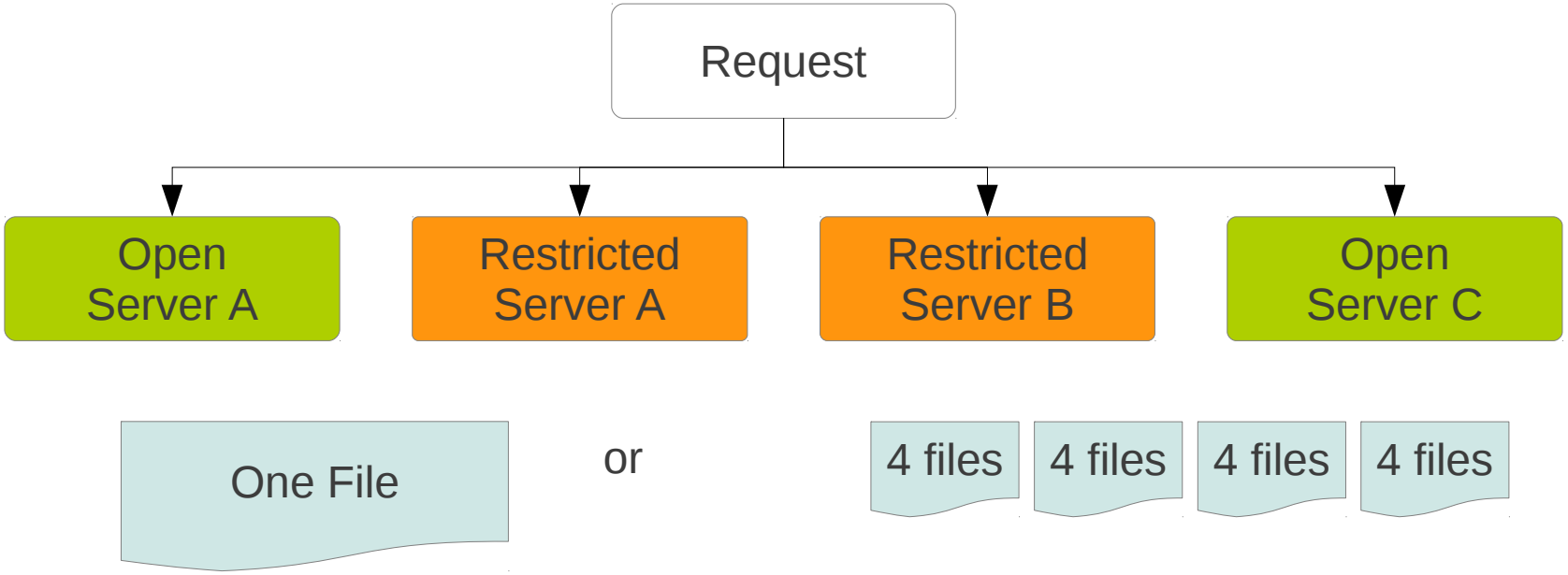
Distributing passwords

- The password will be send by email to the user.
- The password is generated automatically the first time a user request restricted data.

```
Dear User,

This is an automatic message generated by the ArcLink Server at the Bianchi
datacenter. You appear to have requested a seismological data volume that contains
restricted data from here for the first time. From now on, all volumes that you
request from this data center containing restricted data will be encrypted using the
following password:

Your password: PC#tXFDE
Our data center ID (dcid): bia

Please keep it safe for further reference, and prevent other people from seeing it.
Otherwise they will be able to use your identity to obtain restricted data from our
server.

If you use the arclink_fetch tool, please update your dcidpasswords.txt file, by
adding the following line to this file:

bia PC#tXFDE

If you encounter any problems please contact us at: mbianchi@gfz-potsdam.de. Also,
for the correct download of this data make sure you are using arclink_fetch version
2011.221 or newer.

More information at:

 * http://geofon.gfz-potsdam.de/
 * http://www.seiscomp3.org/
 * http://www.seiscomp3.org/wiki/doc/applications/arclink_fetch

Sincerely

Bianchi Team
```

Client Support to Encryption

- arclink_fetch, breqfast were modified to support encryption.
- they will detect the encrypted volumes and save the resulting products in different files if necessary.



- If the user supplied the necessary passwords, the request will be saved already decrypted & merged to the disk.

Enabling encryption on ArcLink

- Configuration file (arclink.ini):

```
...
encryption = true
password_file = <path to the passwords file>*
dcid = "some"
contact_email = owner@somedoamin.org

* default: ${SEISCOMP3_ROOT}/arclink/status/password.txt
```

- Station Bindings / Key files:

```
KEY_VERSION='2.5'
...
ACCESS='someuser@somedomain.org anotheruser@another...'
...
```

Conclusions

- Encryption was added with a minimal changes to the request handler.
- The encryption will not block the download of data, but inhibit its unauthorized use.
- We maintain binary compatibility with IRIS on the encryption schema used.
- We adopted a per-user password on the ArcLink server vs a per-network password adopted by IRIS.
- The passwords on the ArcLink server are stored in a encrypted file on disk, but this could be easily changed to suits individual needs.

Thank you !

Request Handler Protocol

ArcLink Server

```
USER <username> <password>
[INSTITUTION <any string>]
[LABEL <label>]
REQUEST <request_type> <req_id> <optional_attributes>
[one or more request lines...]
END
```

Request Handler

```
RESTRICTED
STATUS LINE <n> PROCESSING <vol_id>
STATUS LINE <n>| VOLUME <vol_id> status
MESSAGE
ERROR
END
```

Status of the request returned by the request handler can be one of:

OK	NODATA	WARN
ERROR	RETRY	DENIED
CANCEL