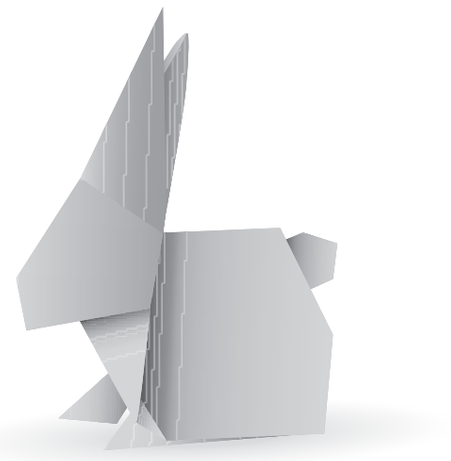
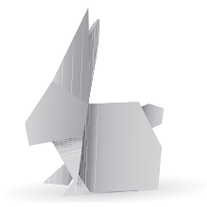
Managing PKI Deployments



WhiteRabbitSecurity

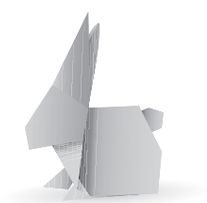
Overview

- Business requirements
- Automated CI/CD process overview
- Demo VM (with Vagrant) (directory layout, usage)
- Modifying the configuration
- Deployment in test environment
- Marking a config package for release and deploying in prod
- Application monitoring and verification with pkicheck



Business Requirements

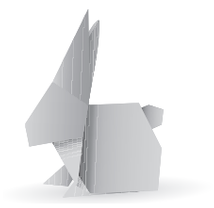
- Lower Costs
  - reduce training
  - automate repetitive tasks
  - standard tools as building blocks
- Higher Quality
  - ease of verification
  - reproducible results
  - reliable test sign-off
  - segregation of duties
  - segmentation from internet for prod systems



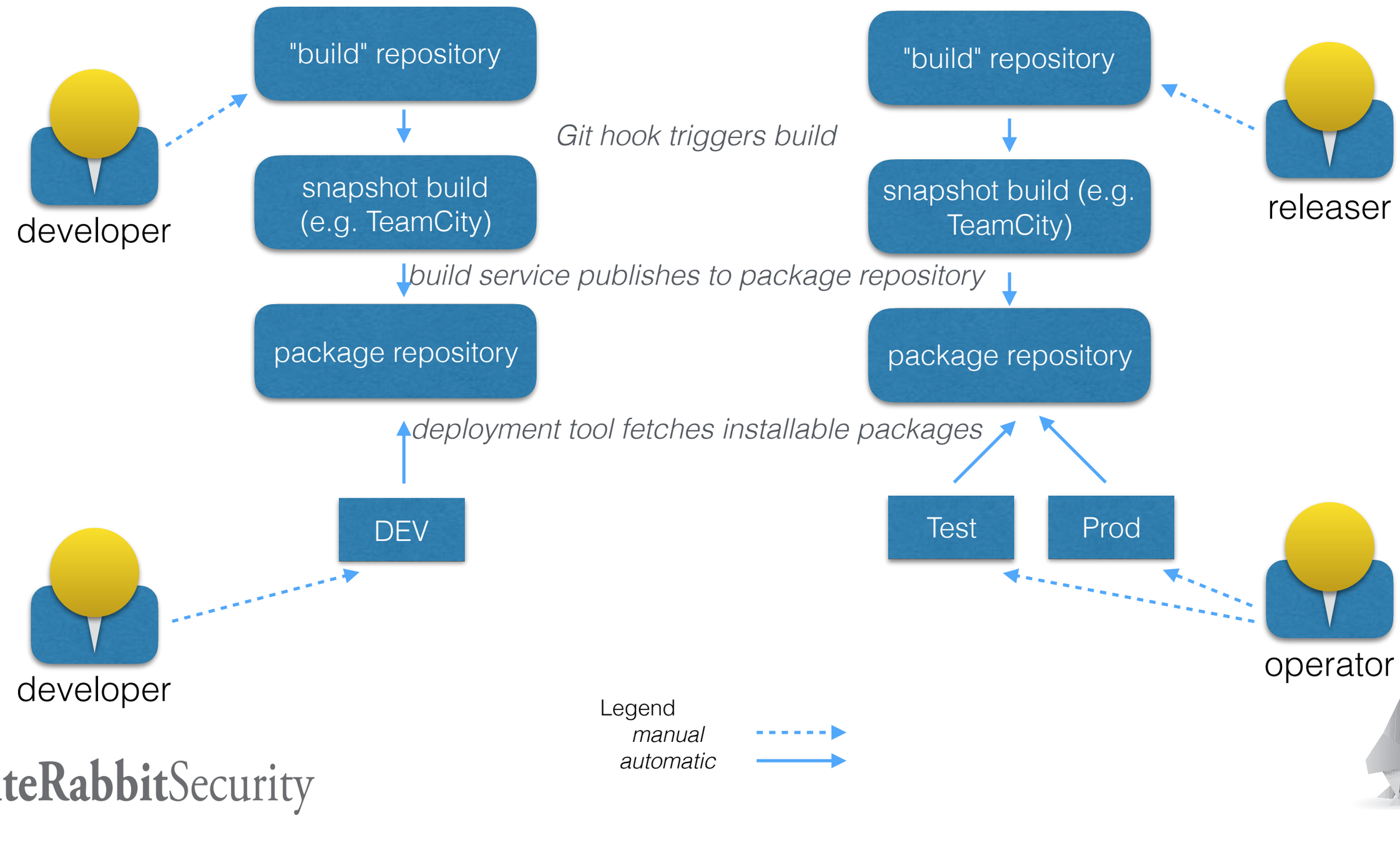
WhiteRabbitSecurity

Packages

- myperl core and supplemental
- openxpki dependencies and core
- additional tools (e.g. pkicheck)
- HSM software, drivers
- openxpki configuration



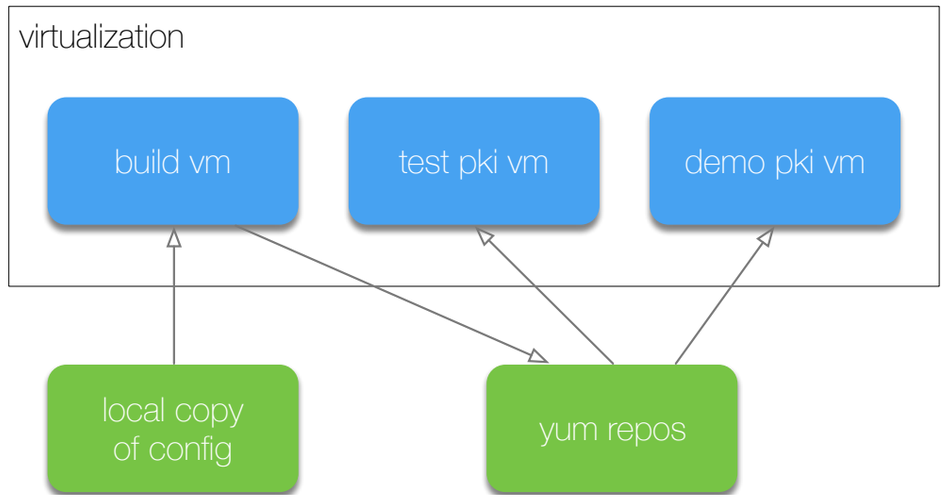
Automated Deployment Overview

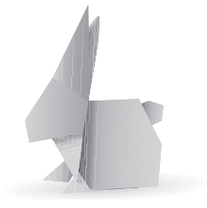


WhiteRabbitSecurity

Our Demo

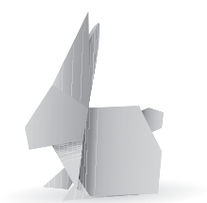
- config modifications done in local working directory "demo-config/"
- "git push" sends update to the "build" VM where the package is built
- "deploy.sh" is run on the "test" VM
- If tests are successful, "release" marks the latest config for production use
- "deploy.sh" is run on the "demo" VM





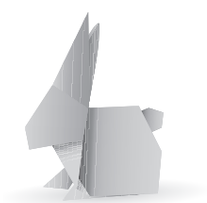
Modify Configuration

```
$ git grep nextupdate config.d/realm/ca-one/crl/default.yaml
config.d/realm/ca-one/crl/default.yaml:    nextupdate: +000014

$ perl -i -pe 's{nextupdate: \+000014}{nextupdate: +000007}' \
> config.d/realm/ca-one/crl/default.yaml

$ git grep nextupdate config.d/realm/ca-one/crl/default.yaml
config.d/realm/ca-one/crl/default.yaml:    nextupdate: +000007

$ git commit -am 'change CRL validity to 7 days'
[demo/master f571aaf] change CRL validity to 7 days
 1 file changed, 1 insertion(+), 1 deletion(-)
```

Build RPM

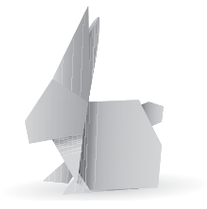
```
$ source ../etc/vgit.rc
$ vgit push build
Counting objects: 7, done.
Delta compression using up to 4 threads.
Compressing objects: 100% (5/5), done.
Writing objects: 100% (7/7), 535 bytes | 535.00 KiB/s, done.
Total 7 (delta 3), reused 0 (delta 0)
remote: INFO: branch=demo/master
remote: INFO: working dir is /tmp/autobuild-8xVv
remote: Cloning into '/tmp/autobuild-8xVv'...
remote: done.
remote: INFO: Running package build (see /tmp/autobuild-8xVv/build.log)...
...
remote: Wrote: /home/vagrant/rpmbuild/RPMS/noarch/openxpki-config-0.1-1805142052.f571aaf.noarch.rpm
remote: Executing(%clean): /bin/sh -e /var/tmp/rpm-tmp.a7kww4
...
remote: Saving other metadata
remote: Generating sqlite DBs
remote: Sqlite DBs complete
remote: INFO: Cleaning up working directory.
To ssh://build/home/vagrant/git/demo-config.git
   c836a86..f571aaf  demo/master -> demo/master
```

pkicheck - OK

```
[vagrant@oxi-test ~]$ sudo /usr/local/bin/pkicheck
/usr/local/lib/pkicheck.d/t/00-basic.t ......... ok
/usr/local/lib/pkicheck.d/t/00-openxpkid.t ..... ok
/usr/local/lib/pkicheck.d/t/00-rpm-v.t ......... ok
/usr/local/lib/pkicheck.d/t/01-tokens-online.t .. ok
All tests successful.
Files=4, Tests=11,  7 wallclock secs ( 0.02 usr  0.02 sys +  1.00 cusr  2.17 csys =  3.21 CPU)
Result: PASS
```

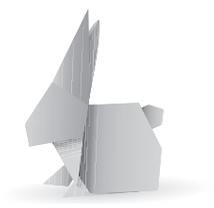
WhiteRabbitSecurity



pkicheck - Not OK

```
[vagrant@oxi-test ~]$ echo | sudo tee -a /etc/openxpki/log.conf
[vagrant@oxi-test ~]$ sudo /usr/local/bin/pkicheck
/usr/local/lib/pkicheck.d/t/00-basic.t ..... ok
/usr/local/lib/pkicheck.d/t/00-openxpkid.t ..... ok
/usr/local/lib/pkicheck.d/t/00-rpm-v.t ..... 5/?
#   Failed test 'Expect no output from 'rpm --verify --nomtime openxpki-config''
#   at /usr/local/lib/pkicheck.d/t/00-rpm-v.t line 23.
#         got: 'S.5......    /etc/openxpki/log.conf
# '
#     expected: ''
# Looks like you failed 1 test of 6.
/usr/local/lib/pkicheck.d/t/00-rpm-v.t ..... Dubious, test returned 1 (wstat 256, 0x100)
Failed 1/6 subtests
/usr/local/lib/pkicheck.d/t/01-tokens-online.t .. ok

Test Summary Report
-------------------
/usr/local/lib/pkicheck.d/t/00-rpm-v.t        (Wstat: 256 Tests: 6 Failed: 1)
  Failed test:  6
  Non-zero exit status: 1
Files=4, Tests=12,  6 wallclock secs ( 0.01 usr  0.02 sys +  0.97 cusr  2.28 csys =  3.28 CPU)
Result: FAIL
```

WhiteRabbitSecurity



pkicheck - Status

```
[vagrant@oxi-test openxpki]$ sudo /usr/local/bin/pkicheck -t json status
[
{"name": "pkicheck", "version": "1.0"}
,
{"version":"1","name":"package","data":{"myperl-openxpki-core":"2.0.3-58","myperl-openxpki-core-
deps":"2.0.3-58","myperl-dbi":"5.24.3-42","myperl":"5.24.3-42","openxpki-
config":"0.1-1805131758.cff7108","myperl-dbd-mysql":"5.24.3-42","myperl-openxpki-
i18n":"2.0.3-58","myperl-fcgi":"5.24.3-42"}}
]
[vagrant@oxi-test openxpki]$
```

WhiteRabbitSecurity