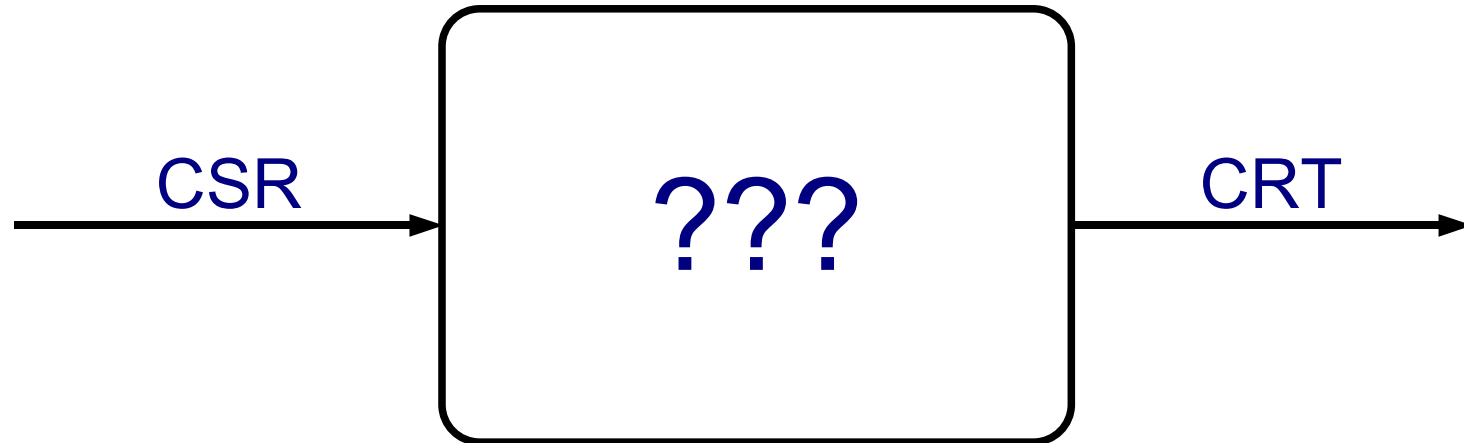
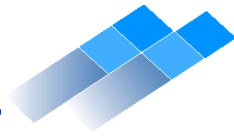


OpenCA Batch System



Oliver Welter - welter@tum.de

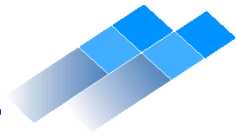


What is the Batch-System

Technical Overview

Default Workflow

Modify/Extend the Workflow



What is the Batch-System

intended use

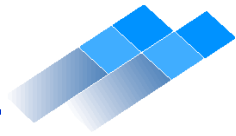
pre-requisites

risks

Technical Overview

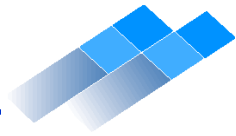
Default Workflow

Modify/Extend the Workflow

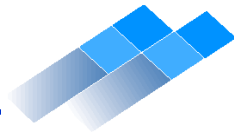


- initial action must be triggered by operator
- no supervision by operator

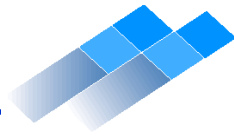
- automated generation of CSRs
- automated signing of CSRs
- automated generation of CRRs
- automated revokation
- automated CRL creation NOT supported



- certificate data
 - pre-processed
 - verified
 - ensured integrity
- appropriate workflow exists



possible
100% integrity loss
if something goes wrong !



What is the Batch-System

Technical Overview

statemachine concept

data storage and import

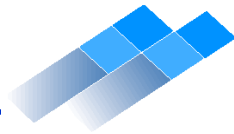
process workflow

process lifetime / batch operation modes

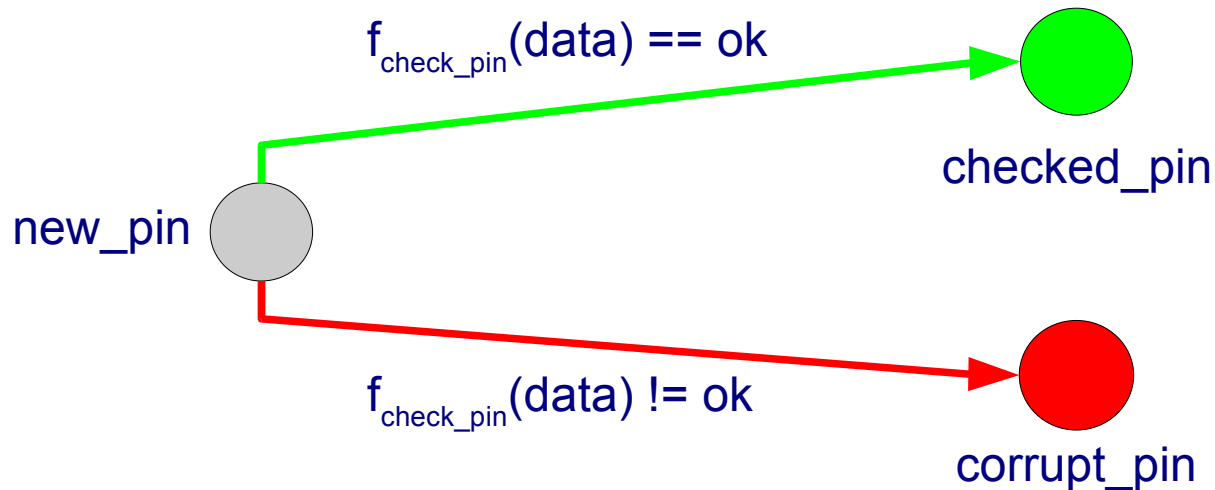
batch function

Default Workflow

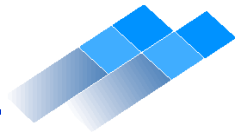
Modify/Extend the Workflow



- defined states
- conditional transitions between states
- current state indicates what function to call next

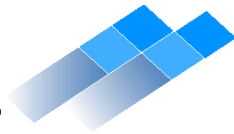


function processes data and sets new state



- batch process / state machine related data on filesystem (var/bp/users/<userid>/<pid>)
- own directory for each process
- file / subdir structure within process directory to store imported and temporary data

- one common directory for data export (var/bp/users/dataexchange)
- **will all move to database with next release !**



```
USER jane_doe
PROCESS hr123
set_state new_process
```

process control

```
ROLE User
SUBJECT CN=Jane Doe, O=OpenCA, C=IT
importedPIN@private
-----BEGIN MYPIN-----
-----BEGIN PKCS7-----
SmXGmDTsQXiRmOvuWWRIgVz3ZjVGRK7fo=
-----END PKCS7-----
-----END MYPIN-----
```

user data

[/j/a/n/e/_/d/o/e/workflows/hr123/](#)

state.txt

data/ROLE

data/SUBJECT

private/importedPIN

statemachine control

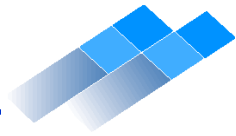
„USER“

„CN=Jane Doe, O=OpenCA, C=IT“

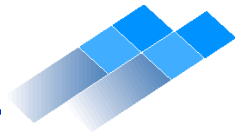
„-----BEGIN PKCS7-----

SmXGmDTsQXiRmO.....

-----END PKCS7-----“



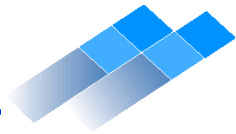
- Look for pending workflows (var/bp/users.txt)
- for all pending workflows:
 - Determine current state (<processdir>/state.txt)
 - Call assigned function
 - new state is written by the function
- above step is repeated as many times as selected via the frontend
- planned: repeat until all workflows reach a stable (or defined) state



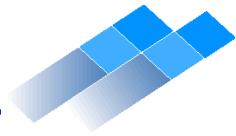
action-based batch mode

- process equal to one workflow (issue cert)
- process is deleted after final state is reached
- new action on same key spawns new process

~~key-based batch mode~~



- transition functions are stored in files
- called within the CA framework
- environment with pointers to
 - global configuration
 - process working directory
 - statemachine control
 - cryptographic tokens
 - log devices
- direct access to the operating system (via perl)
- Future:
 - Batch is only a special OpenXPKI::UI and uses standard core functions
 - Batch operations are accessible with CLI (enables Cron)



What is the Batch-System

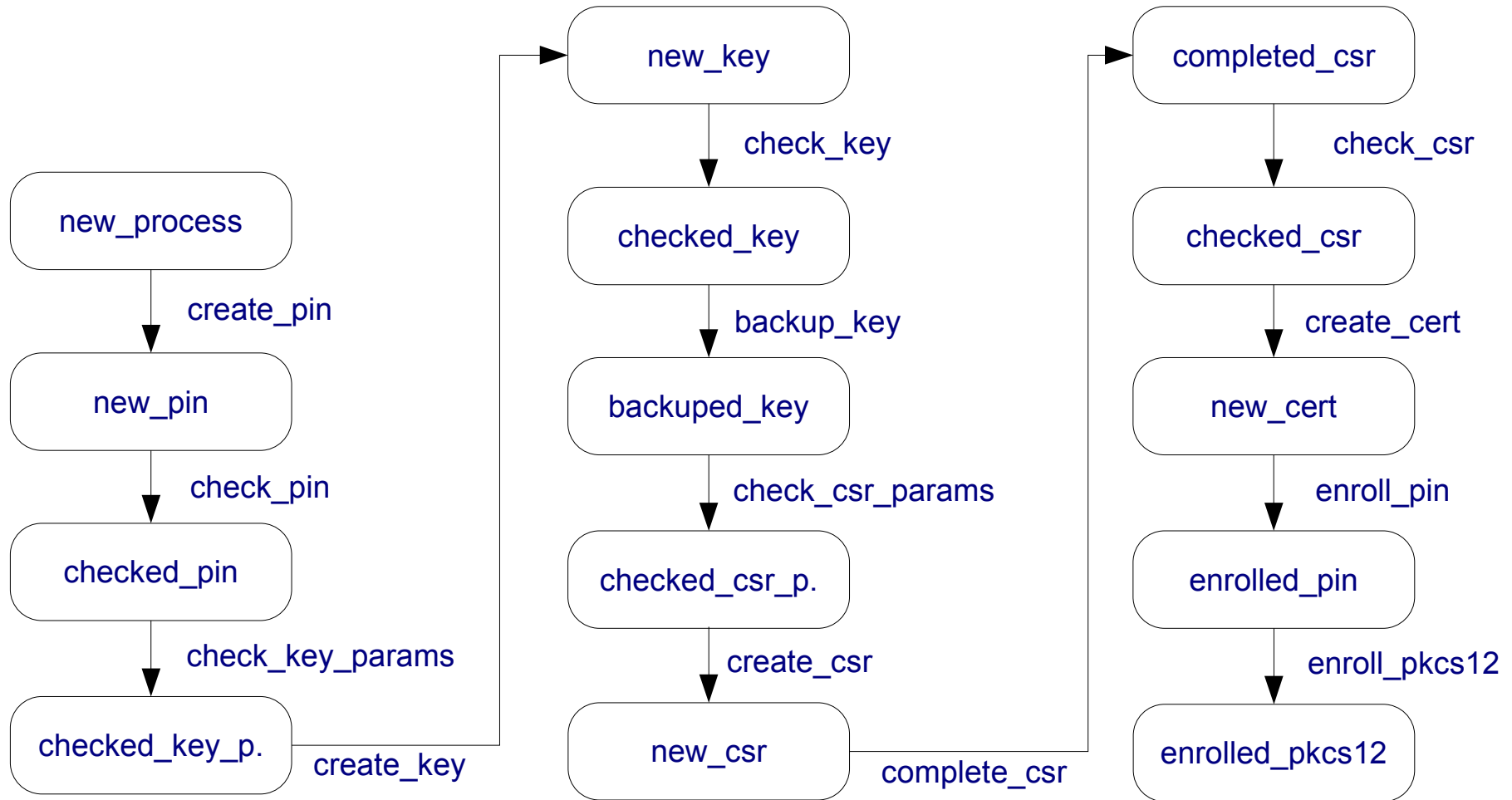
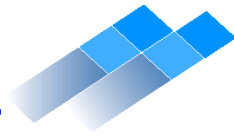
Technical Overview

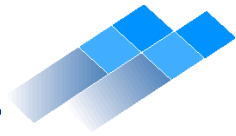
Default Workflow

States

Functions

Modify/Extend the Workflow





What is the Batch-System

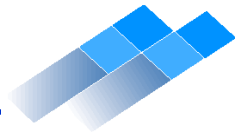
Technical Overview

Default Workflow

Modify/Extend the Workflow

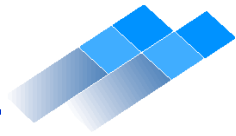
create a new function

bugs, issues, upcoming changes

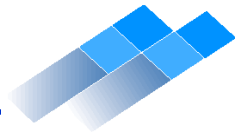


- create a new file lib/bp/myfunction.sub
- import pointers to OpenCA APIs
- implement your functionality
- *use the statemachine-object to set appropriate states*
- add your new states to etc/bp/states.txt

- add the function to etc/bp/functions.txt
- create etc/bp/functions/myfunction.txt and put the possible starting states there



- example batch functions don't use „error-states“
- simple revocation is now implemented
- statemachine accepts multiple states for one process requires resetting the state after processing within the functions (will be fixed in 0.9.3)
- no standard-behaviour for handling enrolled data
- NOTE: Only 32 different states possible (design problem)



- Batch can issue CRLs periodically or via cron
- State-machine based Batch-Processor inside the API
- Batch-Like behaviour via Shell with control outside
- more default workflows (dual key)
- more granular control
- mixed batch/manual operation
- drop all filesystem dependency
- speed up !

protect the environment !

