

OpenCA

... on the road to 1.0

(Michael Bell)

Content

- Today's problems (0.9.2)
- Wishes
- Goals
- Design ideas

Today's Problems (0.9.2)

- Memory leak in the database interface
- No separation of application and presentation logic
- Performance (issuance performance > 10.000)

Wishes

- Cronjobs (CSR-Lists, CRLs ...)
- Better extensibility
- „Unlimited“ Scalability
- CA-Rollover
- Multi-CA Capability

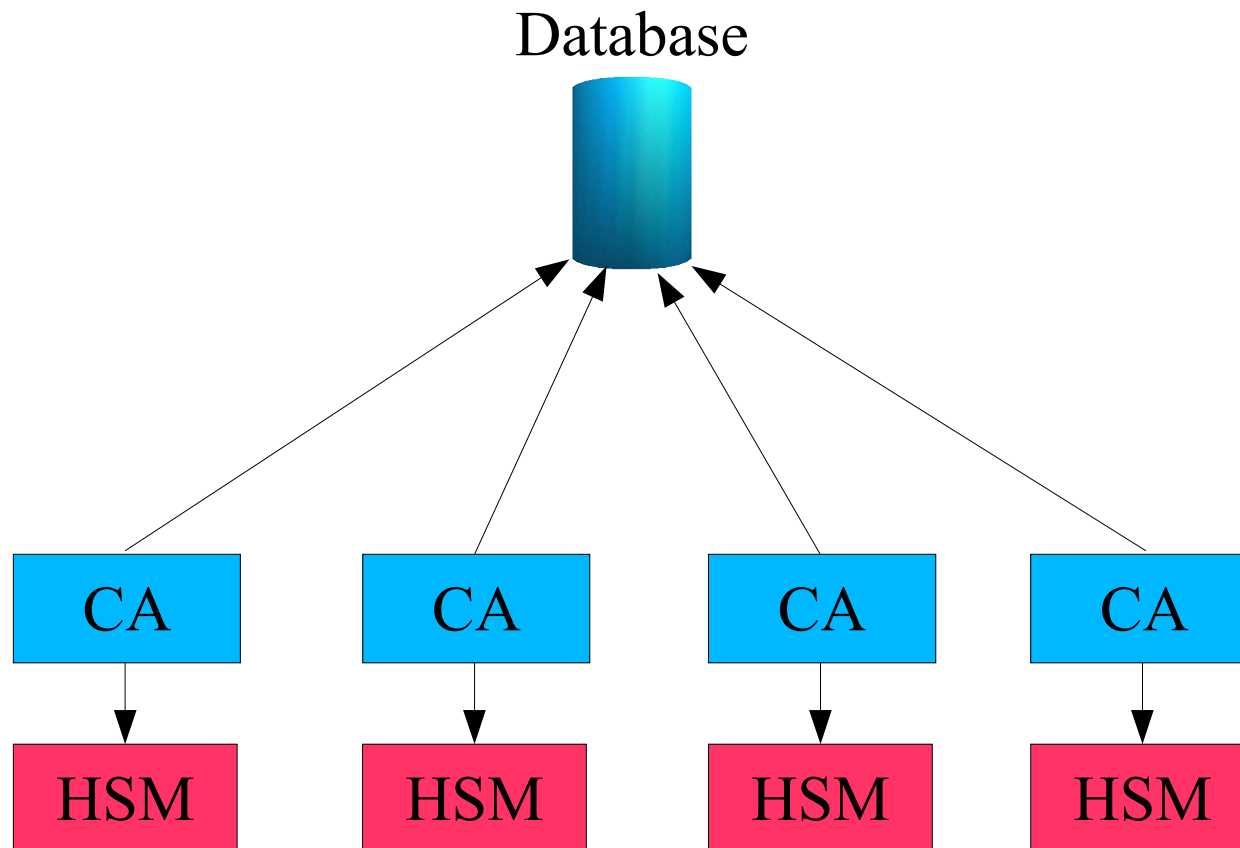
Goals (Core)

- Scalability:
 - Cluster capability of the CA
 - No special OpenSSL files like index.txt und serial (for certificate issuing)
- Extensibility:
 - Core code separate from presentation
 - Modular user interfaces
 - Protocol for OpenCA's filesocket

Design ideas - Scalability

- OpenSSL files:
 - index.txt always empty
 - index.txt for CRLs on-the-fly
 - serial and crl_serial on-the-fly
- Replicated HSMs
- Serialnumbers from Database
- Locks on data objects

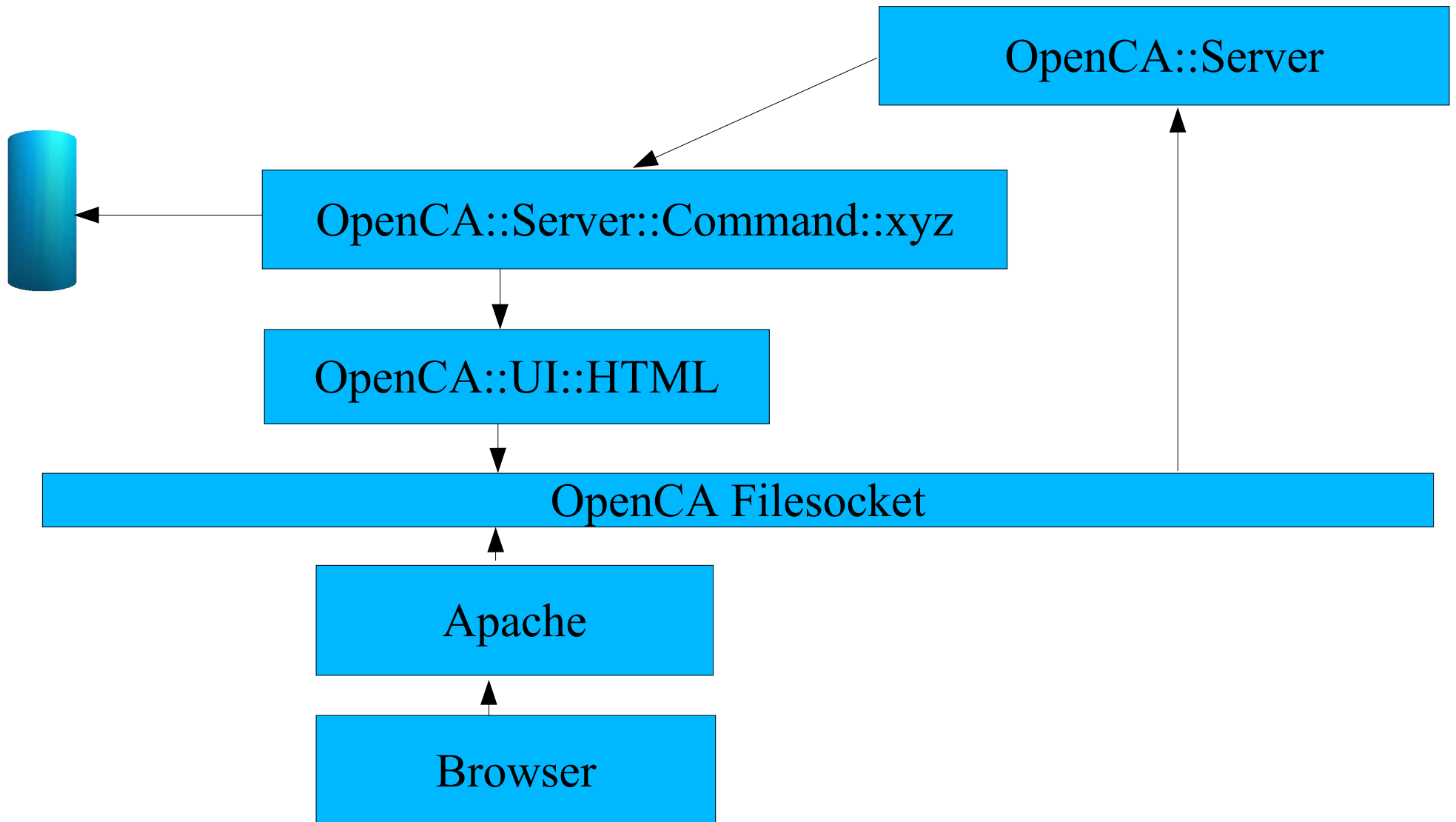
Solution ideas - Scalability



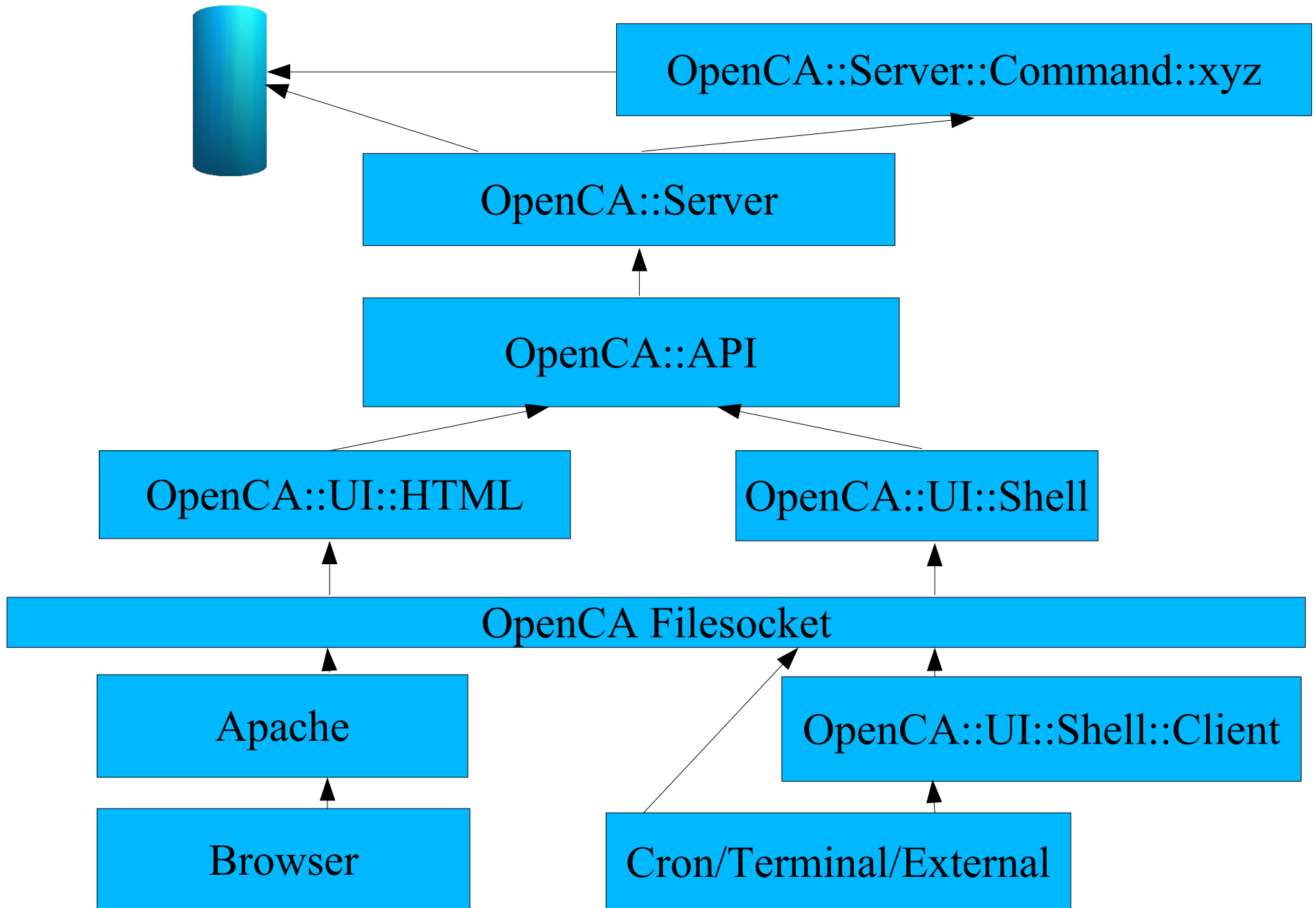
Solution ideas - Extensibility

- Automatic processes:
 - Batch
 - Cronjob
 - API (for other/external systems or GUIs)
- Access control:
 - Multi-person
 - Multi-role
 - Delayed execution

Old Design



Solution ideas - Extensibility



Solution ideas - Extensibility

- `OpenCA::UI::Shell::Protocol` - a real protocol stack
- `OpenCA::UI::*` requires three functions, a part from that no required things
- Full object orientation
- `OpenCA::Server::Command::'`s are all documented

Summary

Everything is going to be alright ...

www.OpenCA.info