libC TECHNOLOGIES

Public Key Infrastructure

libC Technologies SA

Avenue d'Ouchy 18
1006 Lausanne

SwissPKI™

libC Technologies SA
Ave d'Ouchy 18
1006 Lausanne

www.libC.ch
info@libc.ch
T: +41 21 550 1562

libC Technologies SA
Ave d'Ouchy 18
1006 Lausanne

www.libC.ch
info@libc.ch
T: +41 21 550 1562

SwissPKI™

SuissePKI™ is a Public Key Infrastructure which delivers robust hardware based centralized key management backed up by strong cryptography to protect your business processes.

The solution addresses large scale cryptographic key management life-cycle, online hardware-to-hardware key distribution, tamper proof audit as well as usage logs for compliance with standards and covers the complete certificate and key management life-cycle.

SuissePKI integrates with the Primus Cloud or On-Premises HSMs, taking full advantage of the built-in backup and replication mechanisms. Advanced Primus HSM features include securing all keys and PKI meta data objects directly in hardware on the HSM partition.

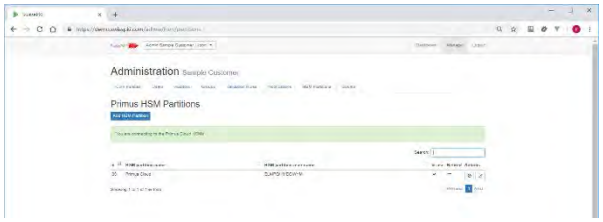
SuissePKI reduces your operational overhead, reduces costs and increases security: no more licensing, maintenance and support of dedicated systems such as database servers, application and archive servers, monitoring and controls systems.

What it does

SwissPKI™ is a feature rich, fully integrated Public Key Infrastructure service which helps expand your enterprise security: from large scale deployments to embedded HSM solutions, the solution provides all necessary out-of-the box components to increase your digital security in a safe, simple and quick way.

Deploy single or complex lattice interconnected Certification Authorities to set up the essential trust between your users and systems. Benefit from our partnership with Securosys SA. Keep your authority keys safe with the Primus Cloud HSM or on dedicated Primus HSMs. Integrates with all major Hardware Security Modules manufacturers.

For a centralized key management with one or two factor remote authentication, high-availability and failover features, SuissePKI™ seamlessly integrates with Securosys Primus HSM. The solution features single or multi-tenant configurations, on premises or cloud deployments as well as single or clustered HSMs.



SuissePKI™ helps you keep your certificates up-to-date and maintain complete visibility over them across issuing authorities. You can assign roles such as registration officer, authorizer or auditor to trusted persons who can manage issuance, renewal or recovery to streamline your organization's work flows to control each certificate management phase. In addition to the certificate policy management available out-of-the-box, you can provide your own micro-services on a policy basis to control misconfiguration, missing fields and/or use internal trusted data sources to validate certificate content.

libC Technologies SA
Ave d'Ouchy 18
1006 Lausanne

www.libC.ch
info@libc.ch
T: +41 21 550 1562

Platforms

SwissPKI is built using a powerful reactive, concurrent, distributed, and resilient message-driven application system.

- ✓ ***Concurrent and distributed systems support***: scale up using resources of one or multiple servers
- ✓ ***Resilient by design*:** self-healing system modules which stay responsive in the face of failures
- ✓ ***High performance***: up to million messages per second on a single machine, small memory footprint
- ✓ ***Elastic and decentralized***: distributed systems without single point of failure. Load balancing and adaptive routing across nodes
- ✓ ***Reactive Streaming Data***: asynchronous non-blocking stream processing
- ✓ ***Automation***: REST interface API for business automation through micro-services
- ✓ ***Interoperability with other services***: Apache, AWS, Azure, Google Cloud, Firebase, JMS

Full featured Swiss Managed Public Key Infrastructure as a Service secured by Primus Cloud HSM. Ready to use and managed by libC Technologies experts. Hosted in Switzerland and certified to the ISO 9001, 14001, 20000, 27001 and 27018 standards.

Full featured Public Key Infrastructure secured by Primus Cloud HSMs for AWS cloud computing customers. Ready to use.

Public Key Infrastructure for Synology including predefined, ready to use certificate policy templates.

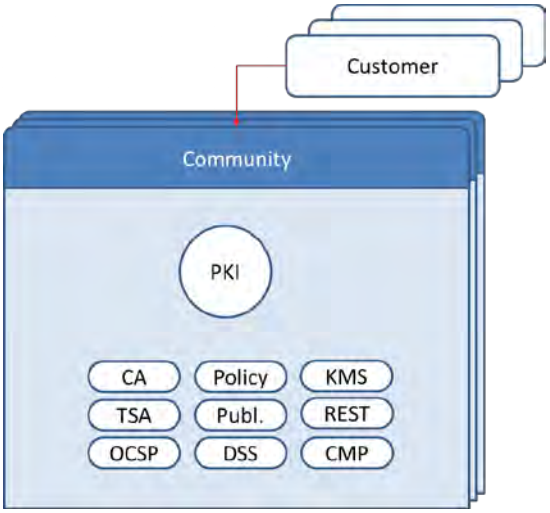
Full featured Public Key Infrastructure on premises secured by Primus Cloud HSM or dedicated Primus HSMs. Container ready.

Appliance SwissPKI all-in-one solution with Securosys SA Primus HSM. The Public Key Infrastructure's secures all key material, X.509 objects, meta data objects and log information on the Primus HSM partitions.

libC Technologies SA
Ave d'Ouchy 18
1006 Lausanne

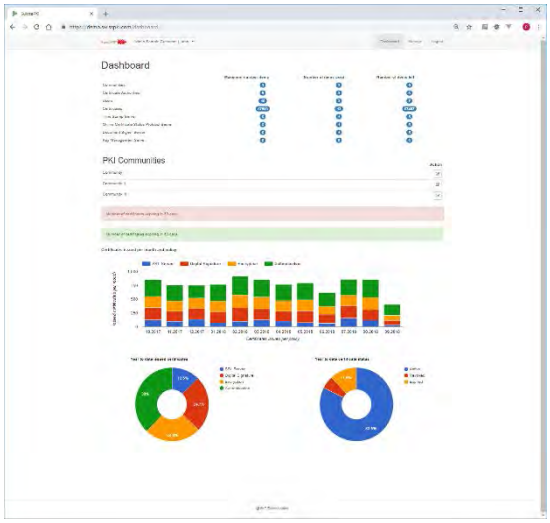
www.libC.ch
info@libc.ch
T: +41 21 550 1562

- ✓ **Multitenant**: create and manage your own customers using ‘customer administrator roles’
- ✓ **Communities**: create and manage PKI communities (e.g. integration, pre-production and production)
- ✓ **Roles**: assign CAO, RAO, Auditor and Authorizer roles to end users (different views per role)
- ✓ **Online:** multiple instances creation and HSM partition assignments using predefined PKI policy templates



Features

- ✓ Multiple Root CA, Sub CA and Cross Signing
- ✓ Certificate and CRL/ARL publisher to multiple destinations
- ✓ Certificate Policy Editor, predefined PKI policies
- ✓ Time Stamp Authority (TSA)
- ✓ Online Certificate Status Protocol (OCSP)
- ✓ Certificate Management Protocol (CMP)
- ✓ Document Signer Service (DSS)
- ✓ Microsoft Certificate Enrollment
- ✓ Certificate Management Life-Cycle Workflow
- ✓ External Public Trusted Certification Authorities



libC Technologies SA
Ave d'Ouchy 18
1006 Lausanne

www.libC.ch
info@libc.ch
T: +41 21 550 1562

Certification Authorities

- ✓ Deploy single or complex lattice connected Certificate Authorities in a few mouse clicks to set up the essential trust between users and systems.
- ✓ Create multiple PKI Communities each supporting multiple certification authorities, certification authority subordination and certification authority cross-signing.
- ✓ Interconnect each certification authority with any satellite component within the PKI community.
- ✓ Manage users using role-based access control: Certificate Authority Officer, Registration Authority Officer, Authorizers and Auditors.
- ✓ Define registration policy templates and assign validation rules to single policy attributes. Publish registration policies to registration groups.

Registration Authorities

- ✓ Register users and systems in a controlled and authenticated manner while applying predefined or custom certification policies.
- ✓ SwissPKI helps you keep track of your registration records through Registration Officer Roles.
- ✓ Create certificate template validation rules using the Certificate Policy Editor and apply run time validations to any X.509 field when issuing certificates.
- ✓ Use pre-defined validation templates or provide your own pre or post validation micro services validate TBS or certificate structure against existing or external data sources.
- ✓ Associate certificate registration policies to registration groups, including list of individual pre and post validators and authorizers if required by your business processes.
- ✓ Advanced REST Service interface for automation.

libC Technologies SA
Ave d'Ouchy 18
1006 Lausanne

www.libC.ch
info@libc.ch
T: +41 21 550 1562

Satellite Services

- ✓ Satellite Services regroup out-of-the box standard X.509 services which you do not need to install and configure separately.
- ✓ The SwissPKI solution integrates compliant Time Stamp Service, Online Certificate Responder (OCSP), Certificate and CRL Publisher and Document Signer Service.
- ✓ Satellite services are part of the SwissPKI as standard modules and deployed, activated or deactivated within seconds by trusted operators.
- ✓ Reduce your operational overhead and take advantage of the turnkey built-in PKI services.

Advanced Certificate Policy Management

- ✓ Create your own certificate policies or use pre-defined certificate policy templates
- ✓ Assign certificate policies to issuing CAs and define which Registration Authority Officer (role) can issue end user or system certificates
- ✓ Define fine grained level validation rules per certificate template attribute
- ✓ Define certificate policy attribute settings: editable, visible or mandatory fields
- ✓ Define certificate renewal rules (manual, automatic) and notification types (multi language)
- ✓ Define authorization rules for individual policy templates
- ✓ Enforce key generation policy (HSM, PKCS#12, PKCS#10, key sizes and algorithms)
- ✓ Include user defined registration information (ID copies or other user/system documents)
- ✓ Comprehensive dashboards providing quick overviews of expiring certificates
- ✓ Advanced certificate search functions and certificate fields and extensions
- ✓ Certificate downloads
- ✓ Certificate publication
- ✓ Certificate revocation (traceability, who, when and why)
- ✓ Manual/automatic certificate renewal
- ✓ Certificate issuance and management supporting external public SwissSign CA

Compliant with standards

SwissPKI supports issuance and management of publicly trusted certificates. Its implementation is governed by the following standards and specifications:

- ✓ "Certificate Issuing and Management Components Protection Profile" defines requirements for components that issue, revoke, and manage public key certificates, such as X.509 public key certificates. The requirements are specified in the Common Criteria (CC).
- ✓ ETSI CAs issuing Qualified Certificates meeting requirements of Regulation (EU) No 910/2014
- ✓ ETSI CAs issuing Web Site certificates meeting requirements of the CA/Browser Forum documents
- ✓ ETSI Other Trust services including time-stamping and CAs issuing certificates other than qualified certificates
- ✓ Mozilla CA Browser Forum Baseline Requirements and Network and Certificate System Security Requirements
- ✓ Swiss ZertES and TAV recommendations

Microsoft CES

Fully automated auto enrolment for Microsoft Active Directory Certificate Enrolment Service to integrate with SwissPKI.

- ✓ Microsoft CES Certificate Enrolment Service
- ✓ Microsoft CEP Certificate Enrolment Policy Service when no Domain Controller is used in the environment
- ✓ Microsoft NDES extension for enrolling devices with password protection

SSH Certificates

Built-in support for SSH Certificates. SSH certificates are not X.509 ASN.1 encoded structure which means that you cannot get them signed by another Certificate Authority. Ideal to setup VPN tunnels to authenticate users and/or hosts. You will not need to copy public keys on thousands of servers when you have the SSH CA public key deployed system wide.

Ad hoc reporting

Integrate optionally with Information Builder WebFOCUS BI Portal. The Portal enables organizations to manage and deploy a wide range of governed analytical content to many types of users, whether inside or outside the firewall.

The Portal incorporates a highly flexible interface for both authors and consumers of analytics. Technical and non-technical authors can very quickly create pages that contain combinations of reports, charts, visualizations, controls and other interconnected widgets. Interact with predefined analytical applications or create your own views and dashboards by dragging content from secure visual folders.