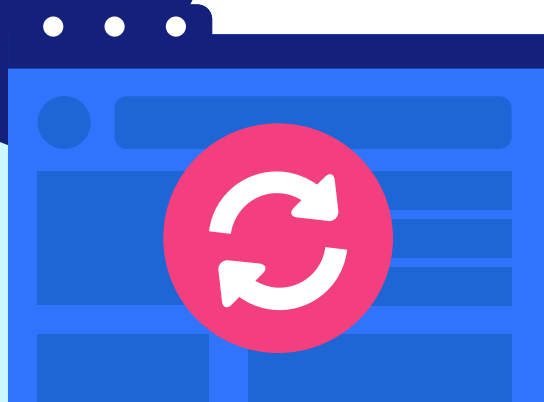
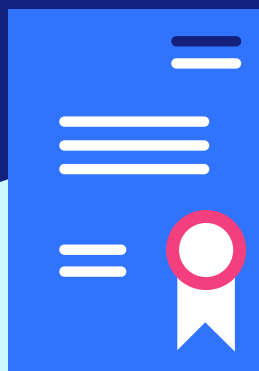


BerryCert

CLM Solution

Certificate Lifecycle Management



digitalberry

www.digitalberry.fr

Digital certificates, also known as public key certificates, are used to identify and authenticate an individual or a machine and to secure exchanges by encryption. They are similar to a digital ID card and have a limited lifespan.

To protect sensitive data and securely connect a growing number of devices, machines and applications, companies depend on cryptographic keys and digital certificates. As a result, there's a surge of these certificates out in the wild, and as a business, it's difficult to manage those certificates using a method such as an Excel spreadsheet.

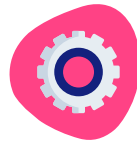


Forgetting to replace one certificate on a single device or server or having a revocation list that you forgot to replace, can take down your entire network.

Consider Microsoft, for example. Teams went down for 3 hours in February 2020 for millions of users, and Spotify's subscribers were unable to access their accounts for more than an hour in August 2020.

SOLUTION BRIEF

BerryCert is designed to let you automatically manage, audit and secure the use of digital certificates in your organization.



Connected to your external and internal PKIs, the solution will provide you with a simple and intuitive interface. It helps you increase security, reduce outages and service interruptions while lessening the charge on your operational security teams.

SOLUTION DESCRIPTION

BerryCert allows:

1

A COMPLETE DISCOVERY of your fleet of digital certificates.

2

CENTRALIZED INTERFACE to manage the certificate lifecycle.

3

AUTOMATIC RENEWAL OF DIGITAL CERTIFICATES

BerryCert is an automated digital certificate lifecycle management and audit solution.



KEY FEATURES AND BENEFITS

- **Complete discovery:** through network and filesystem scanning, PKI synchronization, BerryCert will discover all your issued and in-use digital certificates.
- **Intuitive dashboard:** simple interface to supervise and manage the lifecycle of your digital certificates.
- **Continuous monitoring:** automated expiry alerts and notifications for managed certificates. You will have the ability to schedule a customized reporting process within the solution.
- **Compliance policy enforcement:** compliance analysis of discovered certificates for audit purposes and to ensure the good application of defined security policies.
- **Delegated RA:** BerryCert is your Registration Authority (RA) for your internal and external PKIs. A centralized interface for your certificate issuance and renewal.
- **PKI agility and control:** by automating the certificate renewal and deployment.
- **A tailored solution:** ability to configure your organization's validation and notification workflows for certificate issuance.
- **Easy integration:** BerryCert exposes HTTP web services, intended to facilitate its integration with your in-house applications.
- **Role-Based Access Controls:** ability to define your roles and control access with AD and LDAP or with an IdP via SAML v2 integration. Assign groups and users to certificate lifecycle management tasks from administrators to standard users and auditors.

PRODUCT USE-CASES

- 1. A certificate health-check solution for your infrastructure:** with its discovery and compliance analysis capabilities, BerryCert is your centralized interface for your entire fleet of digital certificates.
- 2. A certificate requests center:** BerryCert is your unified Registration Authority for all your PKIs. All certificate requests are submitted by users and approved by administrators through the solution.
- 3. A risk prevention solution:** service interruptions and certificate outages can jeopardize your business continuity and security. BerryCert will automate the renewal, notify your PKI administrator of the certificates' expiry and record critical activities on your digital certificates.
- 4. A compliance enforcement solution:** BerryCert ensures the good application of the defined compliance policies within your organization. With its scoring feature, the solution will give you a precise view of the conformity degree of all your digital certificates.



EXAMPLES OF SUPPORTED PKIS AND APPS

PKI / APPLICATION	APP TYPE
Smart ID Certificate Manager by Nexus	PKI
EJBCA by PrimeKey	
AD CS by Microsoft	
Digicert	External PKI
Sectigo	
Apache	Application
Microsoft IIS	
NGINX	
Docker Enterprise	
Sectigo	
F5 BigIP Appliance	

SYSTEM REQUIREMENTS

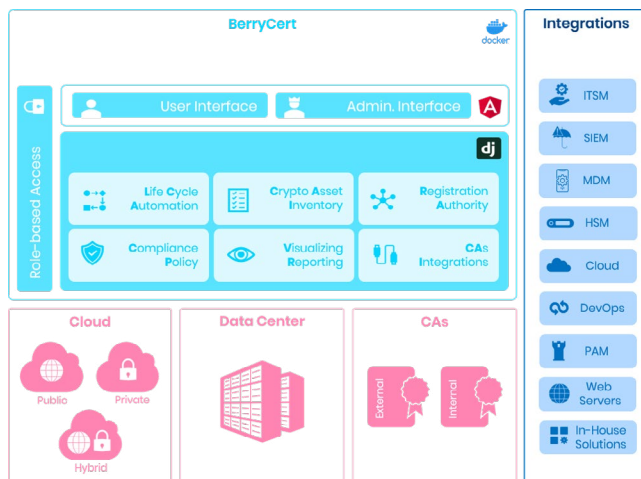
HARDWARE REQUIREMENTS

4 vCPU
 RAM: 16 Go
 Hard drive: 200 Go
 Architecture: 64 bits

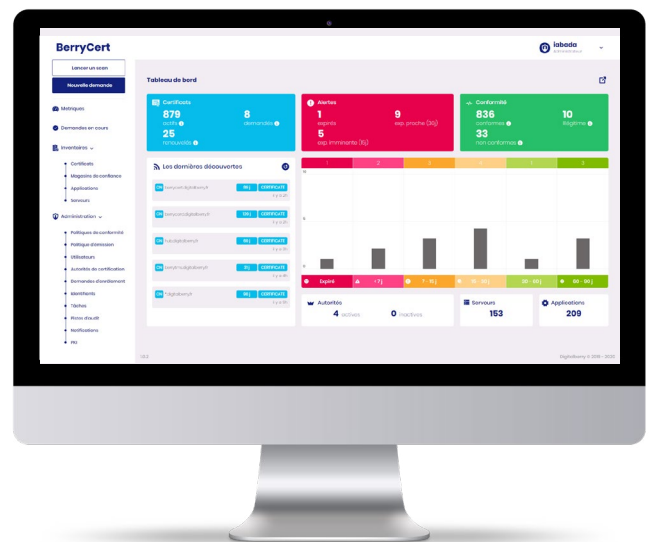
DELIVERY MODE

OnPrem : Virtual Appliance (VM)
 SaaS

BERRYCERT ARCHITECTURE



BerryCert Dashboard



ABOUT

Founded in 2014, Digitalberry is a software publisher operating in the cybersecurity industry. BerryCert, our CLM solution (Certificate Lifecycle Management), helps our customers to reduce their risks of outages certificates by 90%. BerryCert maps, monitors and automates the renewal of all the digital certificates in your information system. We advise and support our customer on their PKI projects within EMEA. Digitalberry has its offices in Marseille and Paris, France and in Tunis, Tunisia."



CONTACT INFORMATION

+33 1 84 19 95 57

contact@digitalberry.fr



www.digitalberry.fr