



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Bertin IT

Website: www.bertin-it.com

Name of Product: Crossing®

Version: v2.2

Date: 29 September 2019 (Revised 27 October 2020)

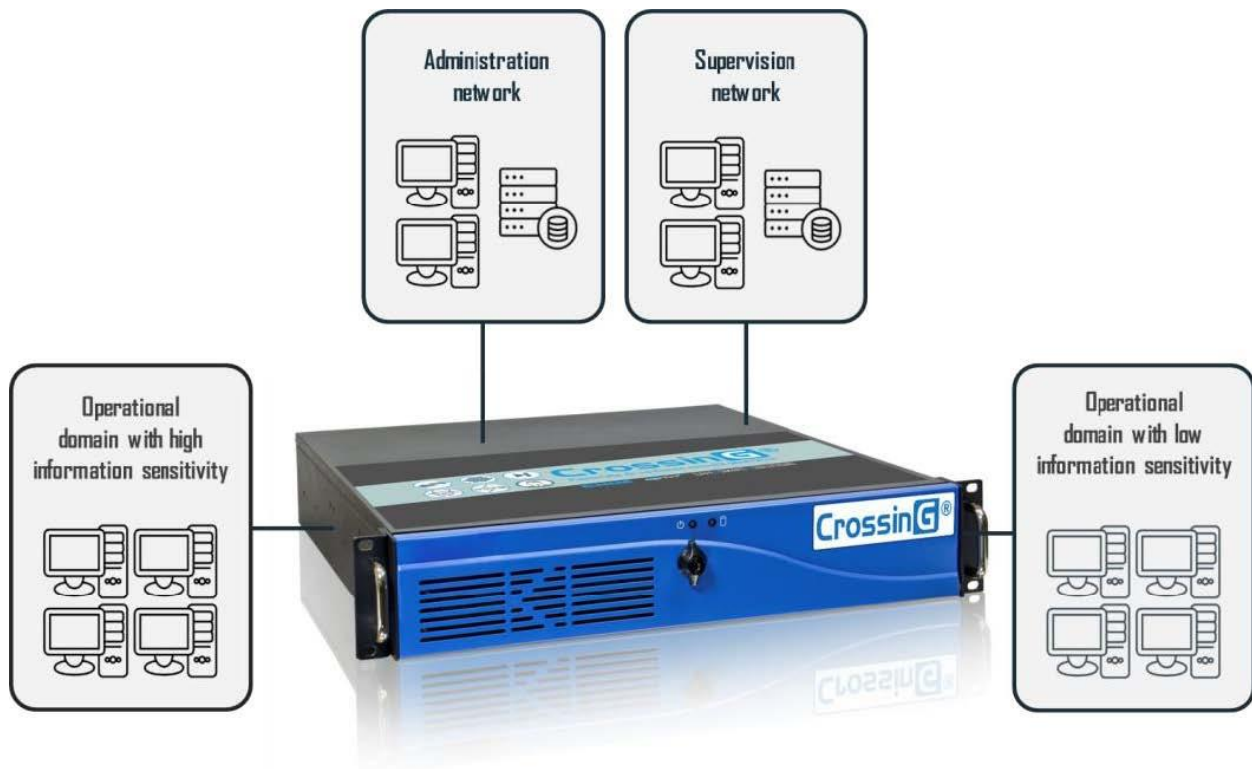
CROSSING® OVERVIEW

CrossinG® is a network partitioning and file transfer security gateway aiming to safely transfer files between networks from different operational domains such as public network (Internet), isolated network (intranet), management IS, Industrial Control System, and more. It particularly enables the implementation of an integrated external exchange system as described in ANSSI's PA-022 note, aimed at operators of vital importance (OVI) and operators of essential services (OES).

CrossinG® works as an access control vestibule as it combines several security mechanisms during file transfer to ensure the in-depth defense of sensitive IS and critical infrastructures. The process aims to first ensure that inbound files are safe and compatible with the company's security policy and then that outbound files are allowed to leave, in order to prevent data breaches.

The product's security policies are defined as an organized set of rules and processes that are applied to the files in order to ascertain whether they are allowed to get in or out. CrossinG® can use two independent unidirectional communication channels, and the gateway can be set either in monodirectional or bidirectional mode. The two-transfer-channel partition allows distinct security policies to be applied depending on the direction of the file transfer.

Although it allows bidirectional exchanges, the gateway provides for each transfer direction a unidirectional internal communication channel and a software protocol break, ensuring a robust partitioning of the networks.



Integration of the gateway in an IS

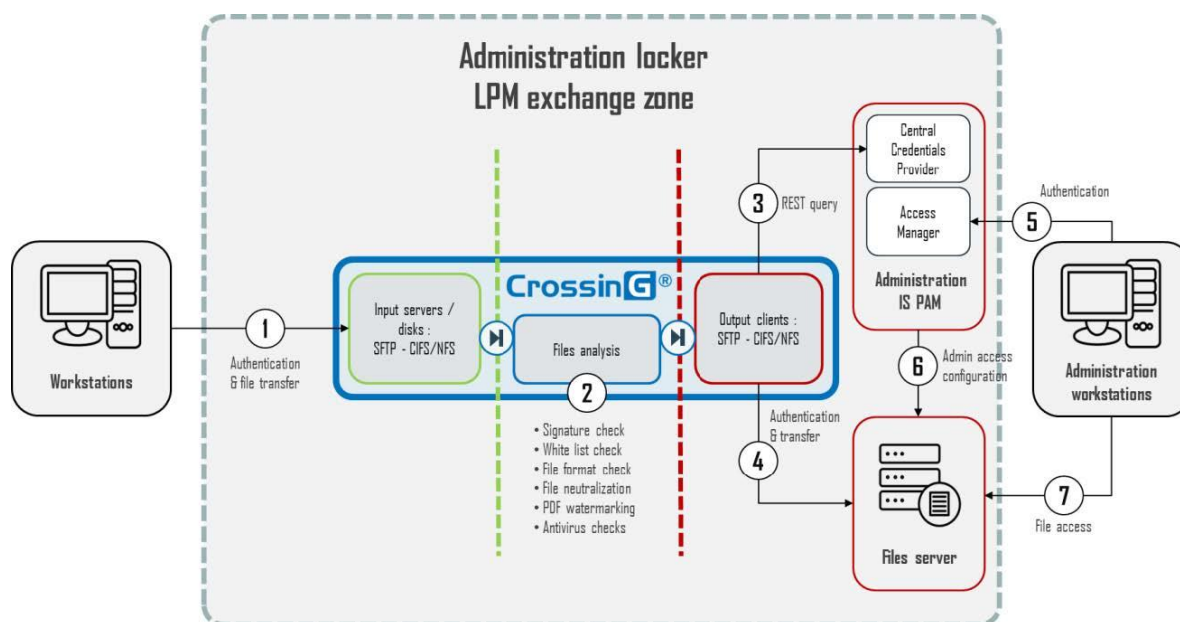
CrossinG® is presented as a hardware appliance (short 2U server). The processing and filtering software chain is included in the hardware platform.

KEY BENEFITS

CrossinG® provides the following benefits:

- Network segregation based enforced by protocol break and internal data diodes (unidirectional software transfer channels)
- File transfer analysis through antiviral checks, white listing of file types (more than 10 000 file types are supported), standard Office, PDF and multimedia files analysis, files signatures verification, PDF watermarking and file neutralization (automated conversion to PDF/A of Office or PDF files) : all these features are customizable by the client through a modern, easy-to-us web interface
- “Multichain” file output based on rules customizable by clients, allowing the routing of the output files to an arbitrary number of servers on the target network according to a number of criteria (such as file name, extension, input protocol, input user name, input LDAP group, and more)
- Support for standard file protocols: SFTP/FTP/FTPS/CIFS/NFS, and user authentication via LDAP/Active Directory

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

CrossinG® segments two networks of different sensitivity. Typically, in the use case of securing an administration network, CrossinG® allows clients of CyberArk who use the PAM on the administration network to securely transfer files from the “unsecure” network to the administration network, while

ensuring that the authentication credentials used on the administration network side are kept under control of the CyberArk PAM.

Neither CrossinG® itself nor Bertin IT provide, install, or configure the PAM functionality. The PAM functionality must be integrated by the client in its network. CrossinG® only provides the means to configure its file clients outputs to retrieve server authentication credentials from the Secrets Manager provisioned by the client in its network.

SECRETS MANAGER INSTALLATION

As mentioned previously, CrossinG® only provides the means to configure its file clients outputs to retrieve server authentication credentials from the CyberArk Central Credential Provider (CCP), provisioned by the client in its network. The Secrets Manager installation is therefore under the client's responsibility.

SECRETS MANAGER CONFIGURATION

The following sections provide details on CrossinG® configuration with CyberArk Secrets Manager.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.

Add Application

Name: BertinIT

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

☐ Access Permitted: From: To:

☐ Expiration Date:

☐ Disabled

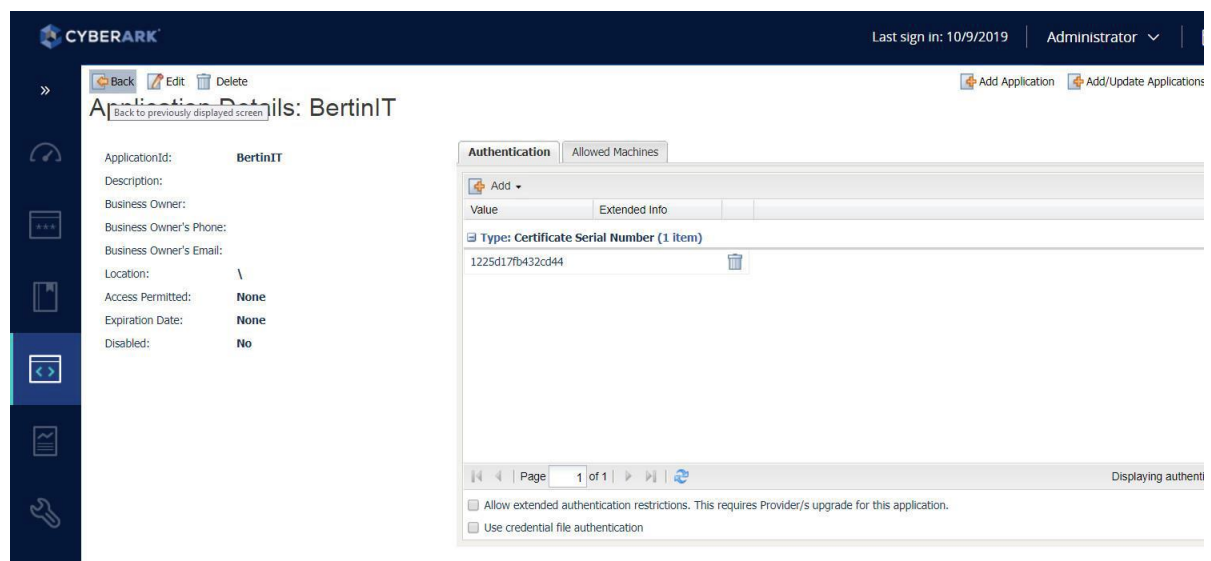
☐ Allow extended authentication restrictions. This requires PAM...

Add Cancel

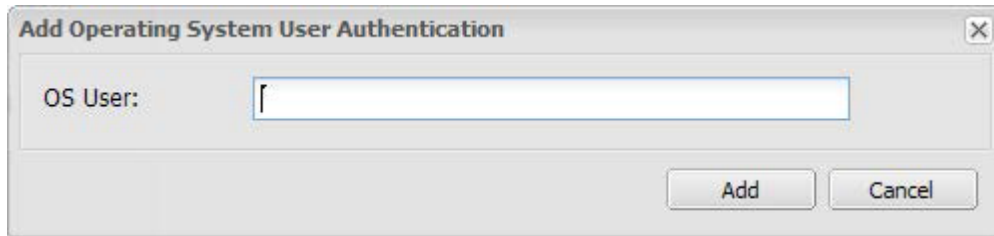
- ☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: BertiniT
- In the **Description** box, specify a short description of the application that will help you identify it.
- In the **Business owner** section, specify contact information about the application's business owner.
- In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.

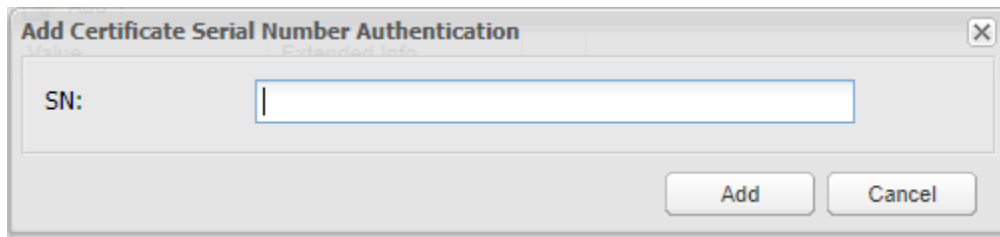
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. Bertini IT suggests customers should use REST APIs securely through the appliance and use certificates. Adding the address of the CrossinG[®] server requesting the credentials to the Allowed Machines, is also supported.
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Select the authentication characteristic to specify.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.



- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Specify the Certificate Serial Number.



Instructions on how to get the Certificate Serial Number:

Windows:

Start -> certmgr.msc (Current User) -> expand Personal -> select Certificates -> double-click on certificate to open

Start -> certlm.msc (Local Computer) -> expand Personal -> select Certificates -> double-click on certificate to open

If the first two options do not work in your env:

Start -> mmc.msc -> File; Add/Remove Snap-in -> Certificates -> Add -> OK -> you may be prompted to choose Local Computer or Current User -> OK

Expand Certificates -> Personal -> Certificates -> Double-Click on a certificate to open.

Once the certificate is open -> Details tab -> Serial Number is in the list of values shown

Once the certificate is open

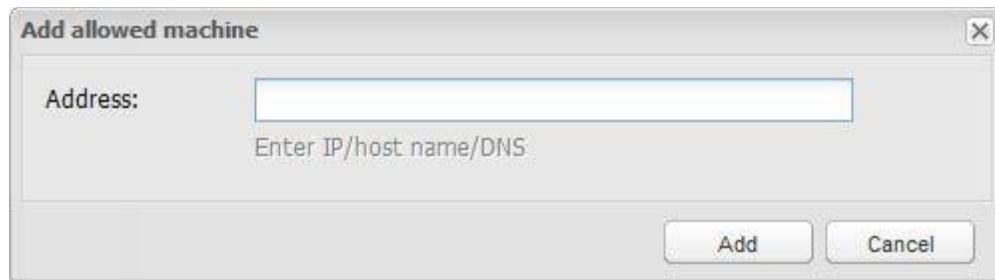
OpenSSL

openssl x509 -in <cert file name> -serial -noout

- This is the most secure way to authenticate the application for CCP

The following are enhanced ways of authenticating

- ☐ Specify the application's Allowed Machines. This information enables Secrets Manager to make sure that only applications that run from specified machines can access their passwords.
 - In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.

A screenshot of a Windows-style dialog box titled "Add allowed machine" with a close button (X) in the top right corner. The dialog contains a label "Address:" followed by a text input field. Below the input field is a hint text "Enter IP/host name/DNS". At the bottom right of the dialog are two buttons: "Add" and "Cancel".

Add allowed machine

Address:

Enter IP/host name/DNS

Add Cancel

- In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

In our specific case, the CyberArk accounts provisioning is performed by the client.

Bertin IT itself does not provide the PAM functionality to the clients, and does not provision CyberArk accounts.

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.

Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the provider user (where the Central Credential Provider is installed) and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ Add the Provider user as a Safe Member with the following authorizations:

- List accounts
- Retrieve accounts
- View Safe Members

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

Add Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☒ View Safe Members

Add

Close

- ☐ Add the application (the APPID) as a Safe Member with the following authorizations:
- Retrieve accounts

☐ If the Safe is configured for object level access, make sure that both the provider user and the application have access to the password(s) to retrieve.

CROSSING® INSTALLATION & INTEGRATION CONFIGURATION

CrossingG® is an appliance that leverages on REST APIs to send a request to the Central Credential Provider to retrieve credentials (username and password), so as to prevent having to store them directly onto the appliance.

For each output rule defined by the gateway administrator, the Crossing® administrator has the capability to select “Authentication par PAM” (i.e. PAM Authentication).

Once selected, a form dedicated to CyberArk REST API can be filled so as to retrieve the appropriate login and password.

Among which:

- The hostname of the Central Credential Provider
- The port to access the CCP

- The path corresponding to the REST API (in case it might be customized by CyberArk or CyberArk client inside CCP)
- The AppID (default is set to BertinIT)
- The Query to be used that matches the target server.
- The CA, certificate and key used to authenticate the appliance onto the CCP

PARTNER CONTACT INFO

Business Contact	Name	Régis Fattori
	Email	regis.fattori@bertin.fr
	Tel	+33 (061) 251-2349
Technical Contact	Name	Vincent Drouin
	Email	vincent.drouin@bertin.fr
	Tel	
Support Contact	Name	Denis Metral-Charvet
	Email	denis.metral-charvet@bertin.fr
	Tel	+33 (060) 765-2814