Smart Card Deployment Models

Introduction

Where smart card authentication is required for authentication to the network or end-user applications, Blue Prism supports a number of operational models to automate the procedure. Typically smart card devices are directly connected to PC's which are used by end users to access the network and applicable systems. Where the Blue Prism Runtime Resources are deployed to physical PCs this same method can be used as each Runtime Resource will have a locally available, physical reader. When following the common method of deploying Blue Prism Runtime Resources to a virtualized infrastructure, the solution requires a different approach.

The deployment models referenced in this data sheet support two smart card authentication scenarios:

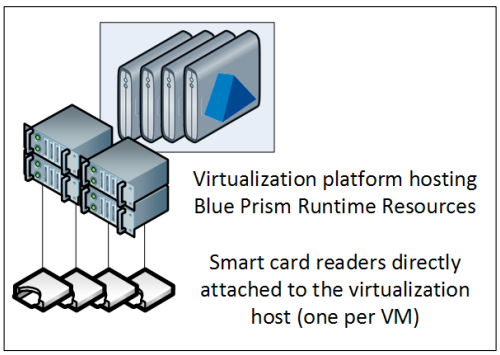
- Manual operator authentication: the Blue Prism controller will manually carry out the authentication on each applicable Runtime Resource prior to initiating the process execution.
- Robotic automated authentication: Blue Prism Runtime Resources are instructed to carry out the authentication as part of executing a process. In this scenario the smart card will be inserted (but not authenticated) prior to the process initiation.

Deployment models

There are two main deployment models which can be used to associate a physical smart card device with a virtualized Blue Prism Runtime Resource.

Local directly connected devices

The smart card hardware (typically a USB device) is directly connected to the virtualization host which, once configured with a series of one-to-one mappings, results in the hardware appearing as a local device on a given guest operating system.

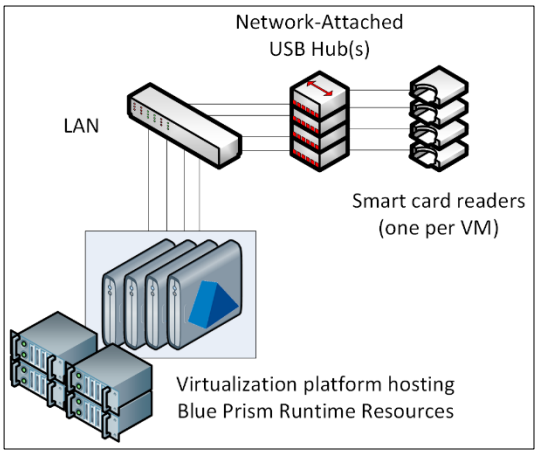


The following features should be considered with this approach:

- Requires the virtualization host to support persistent mapping of USB ports to virtual instances.
- Lower cost as devices are attached directly to the virtualization host. Where more ports are required than are natively provided by the host, additional ports could be provisioned via a directly attached USB hub. This could be limited by the physical space available locally to the server.
- Limited support for disaster recovery scenarios as the devices are physically attached to the virtualization host – therefore if the host is unavailable, even if the Blue Prism components can be recovered elsewhere, provision must be made to re-host the smart card hardware.
- For the manual operator authentication scenario, the operator will require frequent physical access to the virtualization host which may prove challenging from an architecture perspective and present a security risk. Additionally this limitation will require the operator to be located locally to the virtualization host.

Remote LAN connected devices

Network-Attached USB hubs are used to connect the smart card hardware to the Network. When coupled with bespoke USB drivers and utilities, each hub is mapped and configured to appear as a local device on a specified virtual guest operating system.



The following considerations should be applied to this approach:

- Requires specific hardware and software utilities that are able to present the hardware as a local (rather than shared) device to a specified virtualized instance.
- Separation of the smart card hardware from the virtualization host allows controllers to be geographically distributed. This segregation allows the smart card hardware to be secured separately from the virtualization host therefore supporting smart card readers in the same office as the operator whilst the virtualization host is provisioned and secured in a centralized data center.
- A wider range of disaster recovery scenarios may be achieved as the smart card devices are de-coupled from the physical virtualization host.

Selecting a Network-Attached USB device

The following considerations are relevant when choosing hardware to allow smart card devices to be accessible across the network:

- Suitability of the particular USB device for the purpose intended. For example, some products are only suitable for “shareable” USB devices (such as printers and storage devices) whereas a smart card reader is not intended to be shared with more than one target machine.
- How many USB ports are provided, and whether a single device with multiple ports be shared between different virtual machines? A common limitation is that there is often a one-to-one mapping between the device hub and each virtual machine therefore an independent hub may be required for each virtual machine.

AnywhereUSB and Lantronix Ubox are examples of Network-Attached USB Hubs and are named for illustrative purposes only. Blue Prism does not endorse, recommend or imply suitability of any product which may be used to achieve this deployment model, nor has Blue Prism undertaken a market evaluation of any such products.