TTP Introductions
Single authentication to virtualized Windows desktops on shared devices with Citrix and KeyShield SSO

Václav Šamša
KeyShield & SecureAnyBox

Agenda

- The project behind
- What is a shared device?
- A generic or a specific local account?
- Authentication? Why single authentication?
- How KeyShield SSO, Citrix and IGEL work together
- DEMO?
- Q&A

The project behind

- A big hospital with 6000+ employees needed a solution:
  - Shared devices, each for 15+ users within a single shift
  - 2FA with existing chips (used for the access control system)
  - Quick switching between users (NOT Microsoft Fast Switching!)
  - Virtualized Windows workstations preferred
  - 400 physical and 100 installed systems for the first stage
  - SSO everywhere where possible, including blue dinosaurs
- Tender criteria:
  - Functionality
  - Price (TCO for five years)

What is a shared device?

- Mine means – nobody else uses it during the same shift
- Shared means - several users working on the same device during the same shift:
  - Students and teachers (classroom, library, study room etc.)
  - Doctors and nurses, and other healthcare personnel
- Why sharing?
  - Costs
  - Space and short periods of usage

A generic or a specific local account?

- Regardless the shared device runs Windows, Linux or OSX, a local account (profile) must be used – refer to my other session
- If the user works directly on the device with many applications and/or resources, a specific own account works better
- If the user connects to a mission-critical app only or a virtualized desktop, a generic account works far much better
- Please note – the user always works with their identity/account. But own profile is not necessary for it

Authentication? Why single authentication?

- Remote connection to a virtualized workstation needs:
  - Authentication to the device (can be a generic account with autologin)
  - Authentication to the Virtualization system – Citrix, in our case
  - Authentication to the virtualized workstation
- Users are not hired to do any authentication again and again
- Users do their duties = Single authentication is required

Why IGEL, Citrix and KeyShield SSO?

- IGEL fits because they provide:
  - HW box with OS
  - Installable OS
  - OS is IGEL Linux – based on Ubuntu 18
  - Centralized enterprise class management
  - Reasonable pricing
  - Documentation
  - Support (not used in this project, there was no budget for it)

Why IGEL, Citrix and KeyShield SSO?

- Citrix fits because they provide:
  - SAML authentication for both Linux and Windows Storefront clients
  - Virtual Smart Card authentication to virtualized workstations:
    - Combine dedicated CA, AD, MS Kerberos
    - Workstation thinks – there is a smartcard connected
  - Centralized enterprise class management
  - Good local support for the customer
  - Good reputation
  - Still reasonable pricing

Why IGEL, Citrix and KeyShield SSO?

- KeyShield SSO fits because we provide:
  - Windows and Linux client
  - SAML support tested with Citrix
  - Fastest authentication on the planet (not sure about the space☺)
  - HW tokens support for 2FA including the cards they have
  - Support for a wide variety of card readers including the cheap ones
  - Reasonable pricing with concurrent licensing – perfect for healthcare
  - Enterprise class functions incl. Audit, SIEM etc.

How KeyShield SSO, Citrix and IGEL work together?

- IGEL terminal works with a generic account:
  - Account “user“ is automatically authenticated after boot up
  - User has enough access rights to work with KeyShield and Citrix clients
  - User doesn‘t use any other local resources
- File system is read only – reboot means start again from the same point
- KeyShield SSO client is started automatically
- Card reader is connected via USB
- Some devices use 2 readers – for authentication with KeyShield SSO and for authorization with physical Smart card used by doctors

How KeyShield SSO, Citrix and IGEL work together?

- KeyShield SSO is configured to work with 2FA:
  - User must use the card (it‘s contactless – use means touch the reader)
  - User must enter the own AD password
- KeyShield SSO remembers the password – next authentication can be done with the card only (after a coffee break eg)
- Quick user switching works:
  - Logouts the current user
  - Authenticate the new user
- KeyShield SSO client starts scripts after successful Login and Logout:
  - Citrix Storefront client is controlled by commands in the scripts

How KeyShield SSO, Citrix and IGEL work together?

- Citrix Storefront client supports SAML authetication in the same way like MS office for example – tiny browser is a part of the client
- Once the user is authenticated, dedicated CA generates new certificate:
  - SHA signature is stored in AD for MSKerberos lookup
  - The certificate and keys are available through the virtual smart card
  - Must work with same DC as Kerberos
- Virtualized Windows Workstation is configured to work with the Smart Card authentication
- User is authenticate without any manual intervention

How KeyShield SSO, Citrix and IGEL work together?

- Quick user switching doesn‘t shutdown or whatever the virtualized Workstation:
  - KeyShield SSO logout activates disconnect
  - KeyShield SSO login activates reconnection or start and authentication
- When user wants to leave and lock, SHIFT_TOUCH does logout – disconnect from the virtualized Workstation
- When user returns in a while, TOUCH only activates reconnection to the virtualized Workstation
- If another user comes, TOUCH and PASSWORD logouts the previous user and activates reconnection or start of the virtualized workstation

DEMO?

- I‘m very sorry but I our camera man is ill and I can not show you how the IGEL terminal device with KeyShield SSO and Citrix works
- But we are working on a lab installation which will allow me to use remote access to xwindows and show how it works
- I will add demo video to the recorded session when possible

Questions & Answers

Václav Šamša
KeyShield & SecureAnyBox
vsamsa@tdp.cz