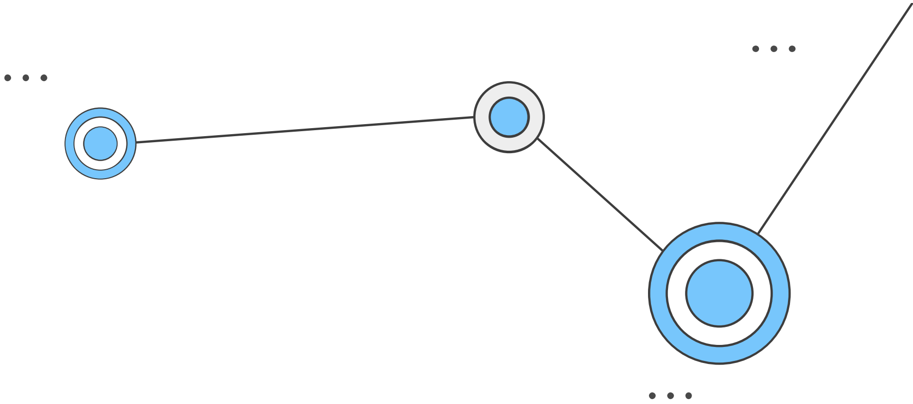
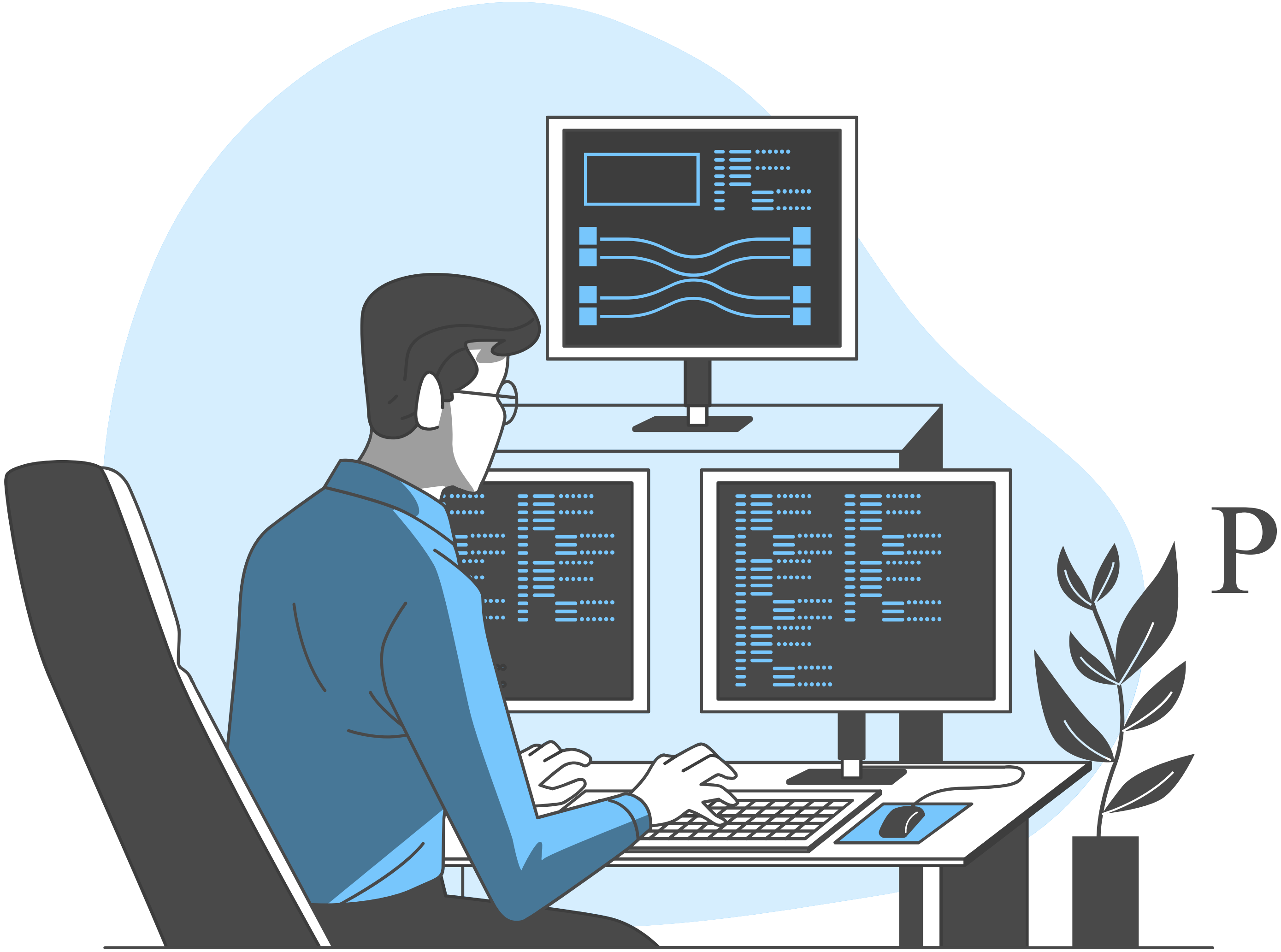




TEAM D PRESENTS

Here is where your presentation begins

01

Digital Signing Requirement in MSIX

Every MSIX package must be digitally signed before it can be installed on Windows.

The signature ensures the authenticity, integrity, and trustworthiness of the application.

Without signing, MSIX installation will fail, as Windows does not allow unsigned MSIX apps.

The signing certificate can come from a trusted public Certificate Authority (CA) or from an enterprise Certificate Authority (for internal apps).

If a self-signed certificate is used, it must be distributed and trusted on all target devices.

Certificate Types

01

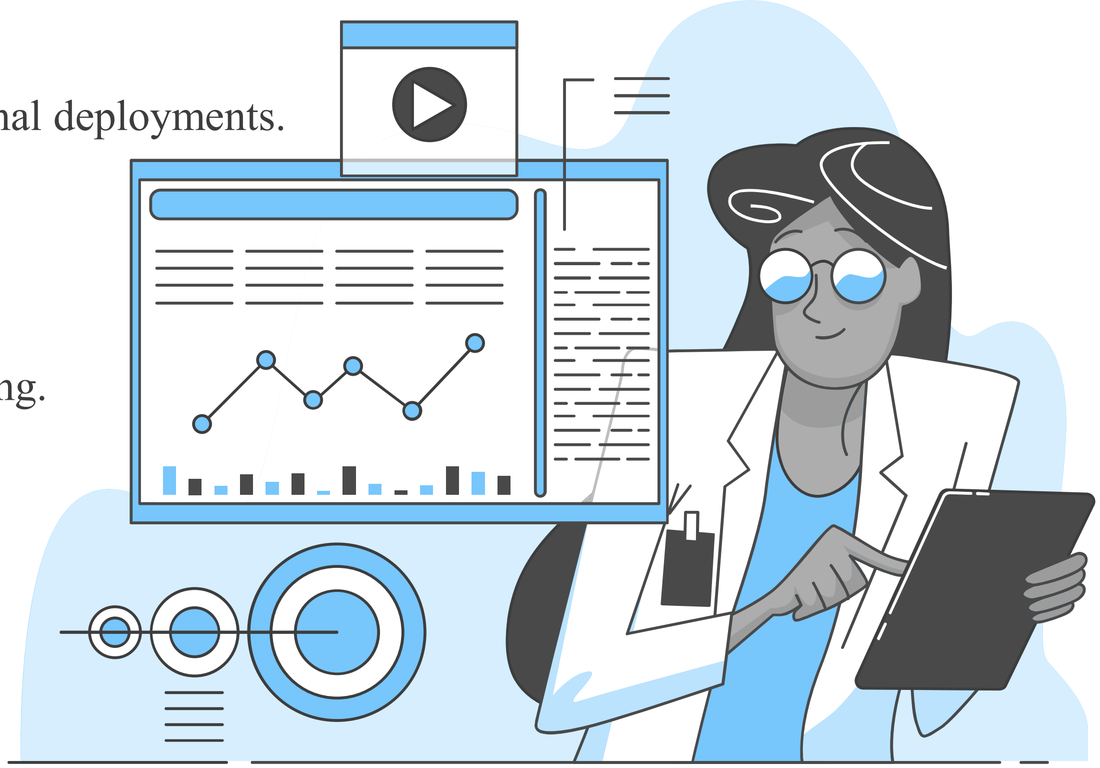
•Public CA Certificate → for Store apps.

02

•Enterprise Certificate → for internal deployments.

03

•Self-Signed Certificate → for testing.



Implementation of Digital Signing

Obtain a Certificate

For enterprise/internal apps, create a self-signed certificate using PowerShell or your internal CA.
For public apps, purchase a trusted certificate from providers like DigiCert or GoDaddy.

Sign the MSIX Package

Use Microsoft's SignTool or PowerShell to apply the certificate to the MSIX file.
This embeds the digital signature, ensuring the package is verified by Windows.

Distribute the Certificate (if needed)

If a self-signed certificate is used, install it into the Trusted Root Certification Authorities store on all client devices.
This can be automated using Group Policy (GPO), Intune, or manual import.

Verify the Signature

After signing, validate the package using SignTool or PowerShell to confirm that the MSIX is correctly signed.
Only signed and verified MSIX packages can be installed without errors.

2

Troubleshooting Tools for MSIX Packages

- **Event Viewer** → Check *AppxDeployment-Server* logs for install errors.

- **PowerShell Cmdlets** –
- Add-AppxPackage (manual install with detailed errors)
- Get-AppxLog (fetch error details)

- **Signtool.exe** → Verify package signature & certificate validity.

- **MSIX Packaging Tool** → Validate and repackage apps.

- **Process Monitor (ProcMon)** → Deep dive into file/registry access issues.

… … …

- **MSIX Hero** → Inspect package contents, dependencies, and manifests.

3

Preparing Infrastructure for Desktop Management (SCCM)

- **Install & Configure SCCM Environment**
- Set up SCCM site server & site database.

- **Enable Active Directory Integration**
- Extend AD Schema & configure System Management container.

- **Configure Boundaries & Boundary Groups**
- Define network locations for device discovery & content distribution.

- **Client Deployment Preparation**
- Enable client push installation, group policies, and certificates.

- **Distribution Points & Management Points**
- Deploy content and enable client communication.

- **Security & Compliance**
- Configure roles, permissions, and PKI if required.

4

Managing the configuration manager Client

01

Monitors client health and activity.
Runs client actions (Policy Retrieval, Inventory, Software Updates)

02

Troubleshoot issues using logs and built-in tools

03

Client reset or reinstallation if required

04

Reporting and compliance monitoring in SCCM console

1.Configure communication settings (HTTP/HTTPS)
2.Assign site (Automatic or Manual)
3.Apply client policies (software updates, inventory, endpoint protection)
4.Schedule hardware/software inventory scans
5.Enable automatic client health evaluation and remediation

5

Managing inventory for PCs and applications

Hardware Inventory

Collects details about PC hardware.

Examples:

CPU, RAM, Disk space
BIOS, Firmware, Serial number
Network adapters, IP addresses
Installed drivers
Helps in capacity planning, asset management, and troubleshooting.

Software Inventory
Collects details about files and executables on devices. Tracks software usage (optional).

Examples:
Installed applications
File versions and locations
How SCCM Collects Inventory
1. Client Agent runs on each PC.
2. It sends inventory data to the Management Point (MP).
3. MP forwards it to the SCCM site database.
4. Admins can view reports in the SCCM Console or SSRS reports.

THANK YOU SO MUCH