XPCM

Cross

Platform

Credentials

Management

…for all your scripts!

Get-SpeakerInfo -Brief

Meta: {Evgenij Smirnov, B.Sc. Physics, 1972, Berlin}

Twitter: @cj_berlin

Blog: { https://it-pro-berlin.de, https://metabpa.org }

Employer: DTS Systeme GmbH

User Groups: {Windows Server UG Berlin, Exchange UG Berlin, PowerShell UG Berlin}

Certs: {MCSE, VCP, VCIX, QCIC, CCA, ITIL, …}

TechNetPoints: 52165

Publications: -gt 100

SpeakerAt: {PSConfEU 2019+2020, CIM Lingen 2018+2019, PSDAY.UK}

Awards: {MVP CDM 2020}

MISSION STATEMENT

Design and develop a

- **simple & robust**
- **manageable**
- **secure**
- **cross-platform**

solution to provide credentials to PowerShell scripts.

…so is this going to be yet another talk about the SecretManagement module?

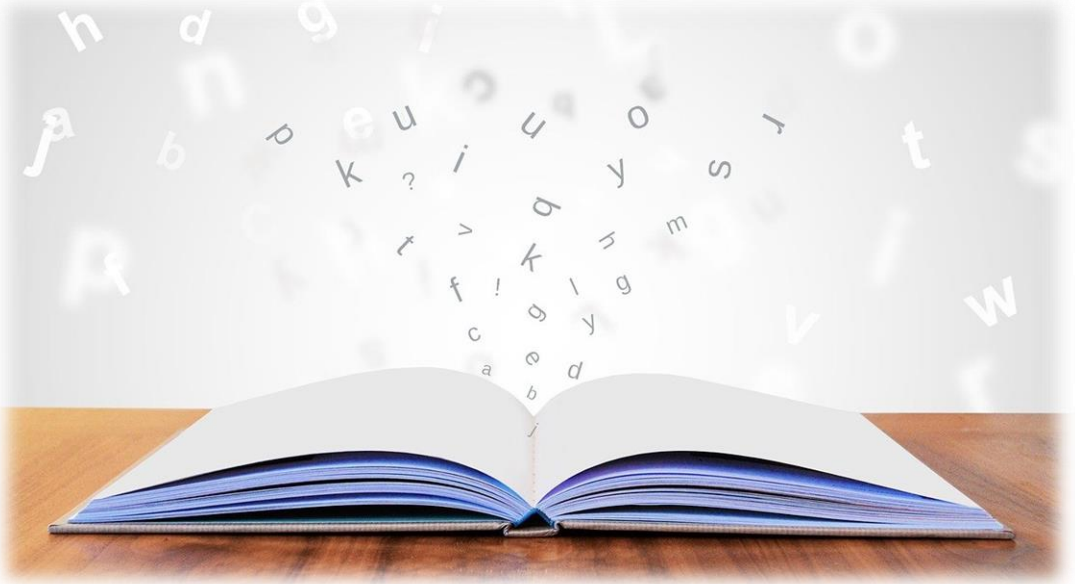
Nope ☺

WHAT'S WRONG WITH SECRETMANAGEMENT?

- **It's not there (yet)**
  - We're still in Preview
  - Breaking changes (module rename) were introduced between preview releases
  - Binary module so no easy code review possibility for scripters
- **It's not cross-platform (yet)**
  - PowerShell team is committed to release a cross-platform version
  - However, backwards compatibility to 5.1 is arguably more important
  - Vault connectors may or may not be cross-platform
- **Code quality is not guaranteed where it matters most**
  - The only connector coming from Microsoft is not centralized, nor cross-platform
  - Everything else is 100% community-developed

PROVIDING CREDS VS. USING CREDS

- **No matter how securely we provide a set of credentials to a script…**
- **…there is nothing to prevent the script‘s author from disclosing or abusing them.**



- **So, if *you* are the script‘s author, don‘t be evil:**
  - Scrub any variables containing secrets the moment they‘re no longer used
  - Remember that on non-Windows OS a SecureString is not encrypted
  - Do not expose credentials unnecessarily, e.g. by passing them via HTTP GET without SSL or persisting them in cleartext in a file.

DEMO

SecureString on Linux

SUCCESS CRITERIA

- **Done with what‘s in the box**
  - No fancy compiled 3rd party stuff that updates from the Store and requires telemetry!
- **Onboarding of a node with as little interaction with the node as possible**
  - Ideally, no interaction should be necessary – this won‘t always be doable…
- **Updating a secret causes as little work as possible**
  - Ideally, a password change should only require one action
- **No „crown jewels“ component (one master key unlocks everything)**
  - No component should hold the secrets in plain text (or equivalent)
- **As little hardwired naming as possible**
  - If the central infrastructure changes, the scripts should be still able to get their secrets

ENTER CMS

- **Described in PKCS#7 (RFC5652 = CMS 4.0)**
- **Only the target node holds the decryption key**
- **Content-agnostic: Will encrypt anything, as long as it‘s a byte array**
- **Native PowerShell support (*at least in 5.1*)**

- **Certificates can be obtained by nodes through autoenrollment, the public part can be read from the CA (*zero-contact onboarding*)**

DEMO

CMS in action

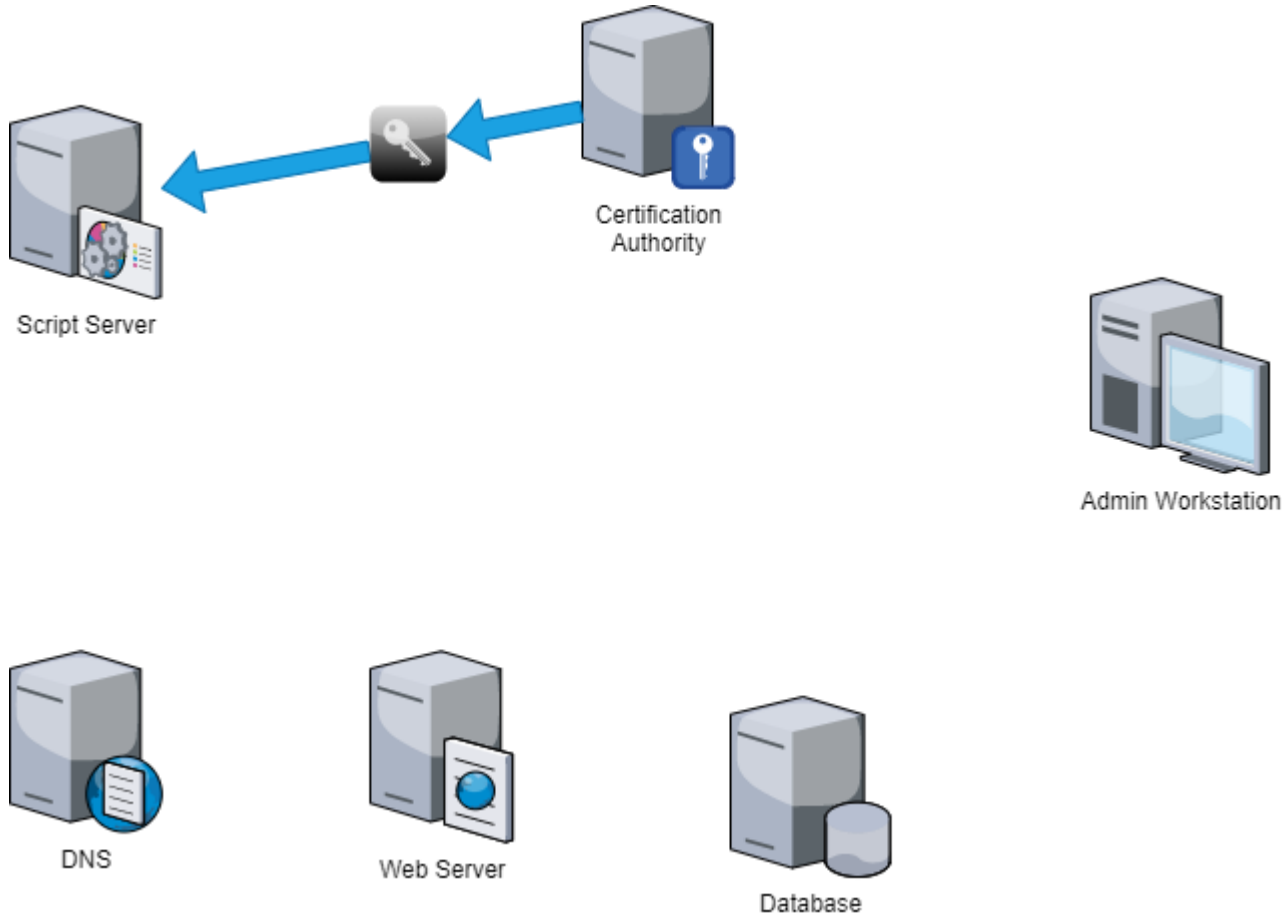
CMSMESSAGE & LINUX

- ***-CMSMessage cmdlets are not (yet) available on Linux (or MacOS)…**
  - They‘re present in the current 7.1 preview – happy days ;-)
- **… but the underlying .NET circuitry is…**
- **…and it works on Windows as well!**

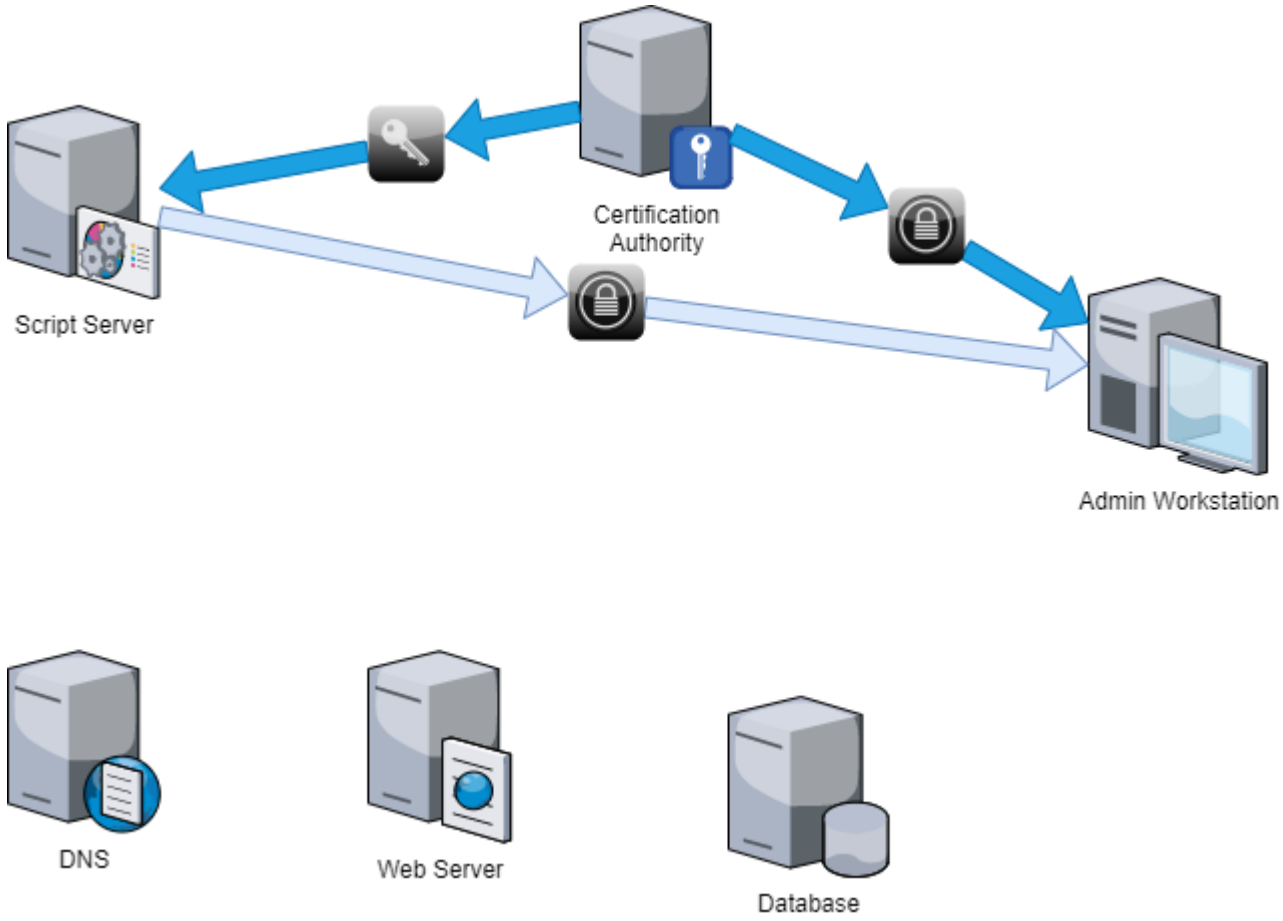
DEMO

CMS across platforms

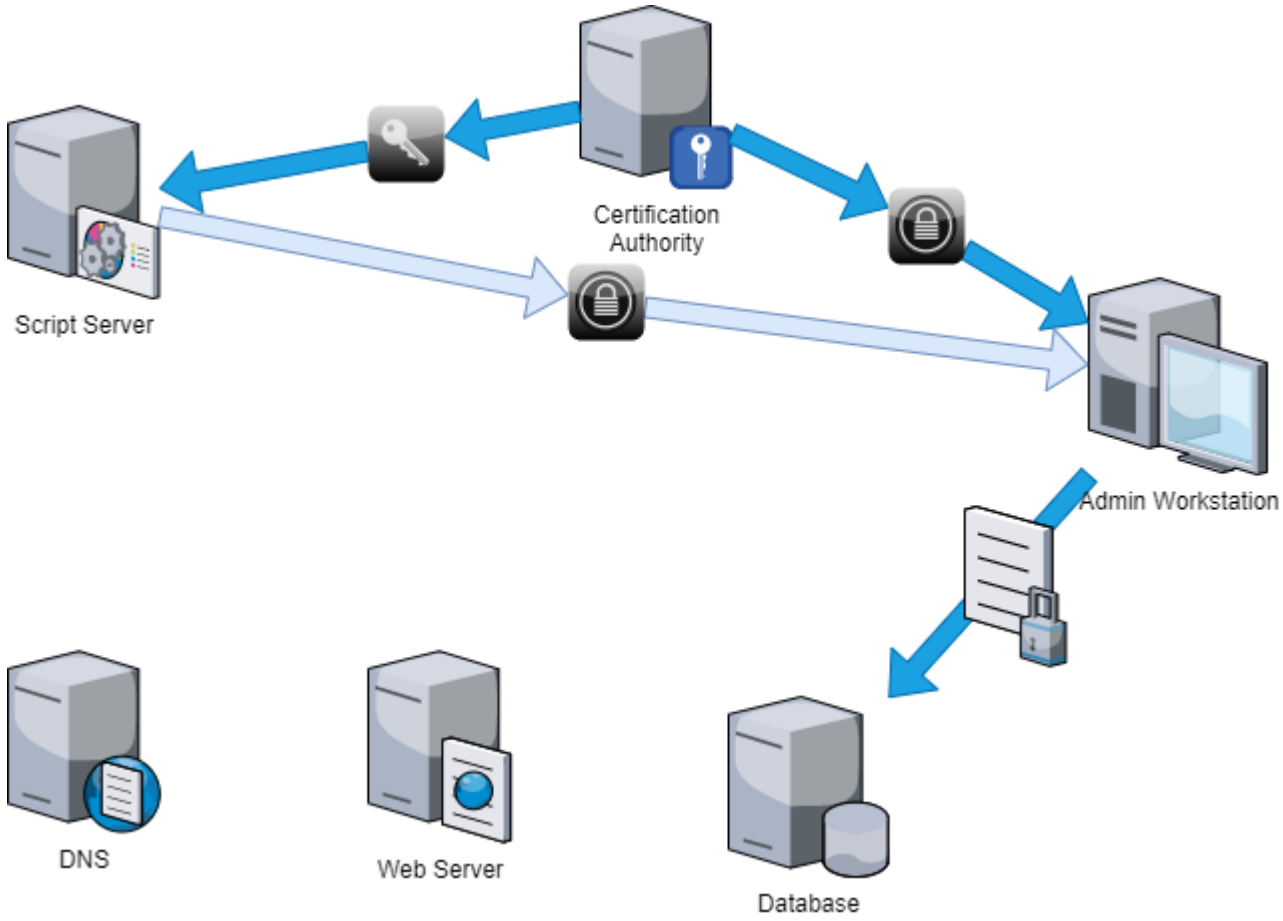
THE PLAN



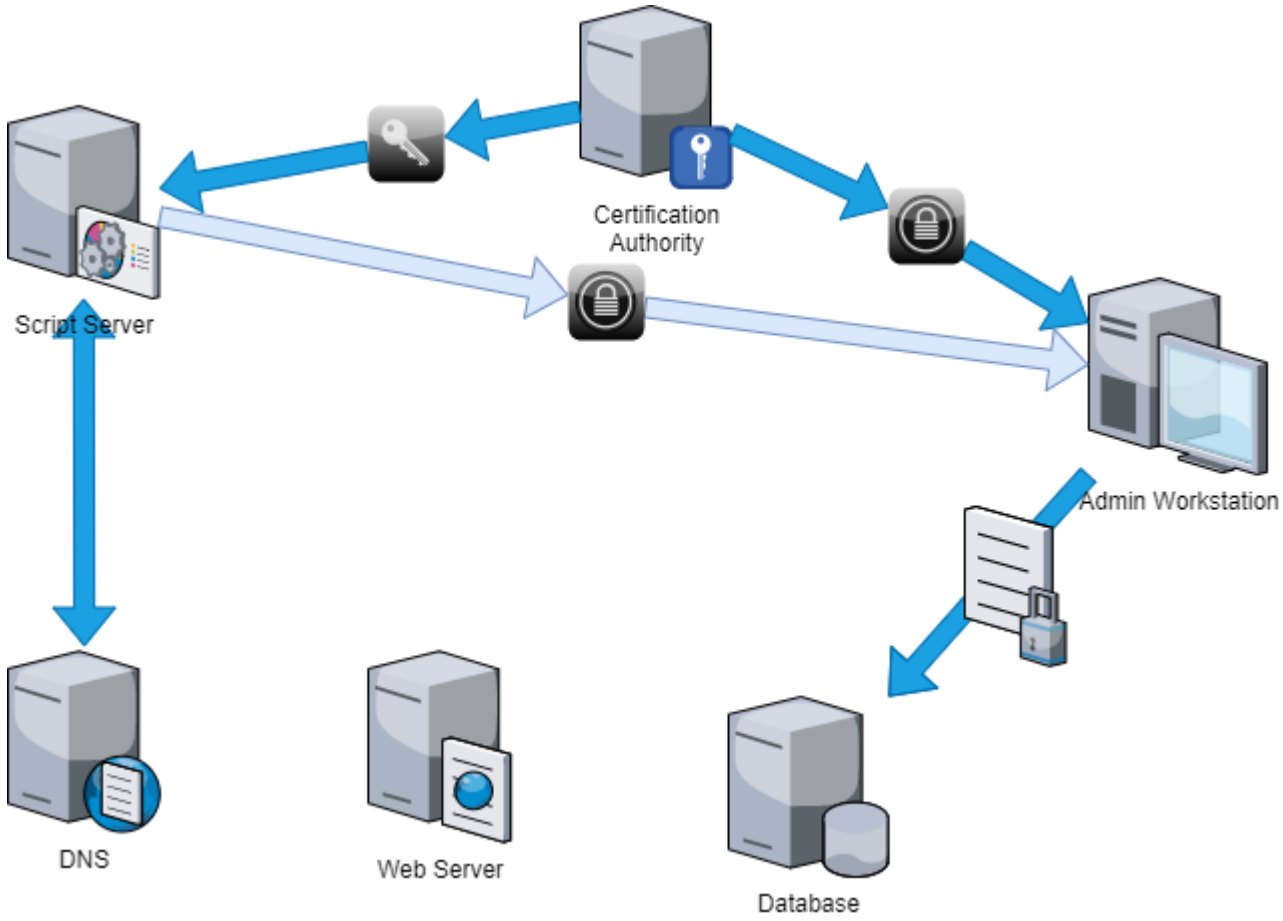
THE PLAN



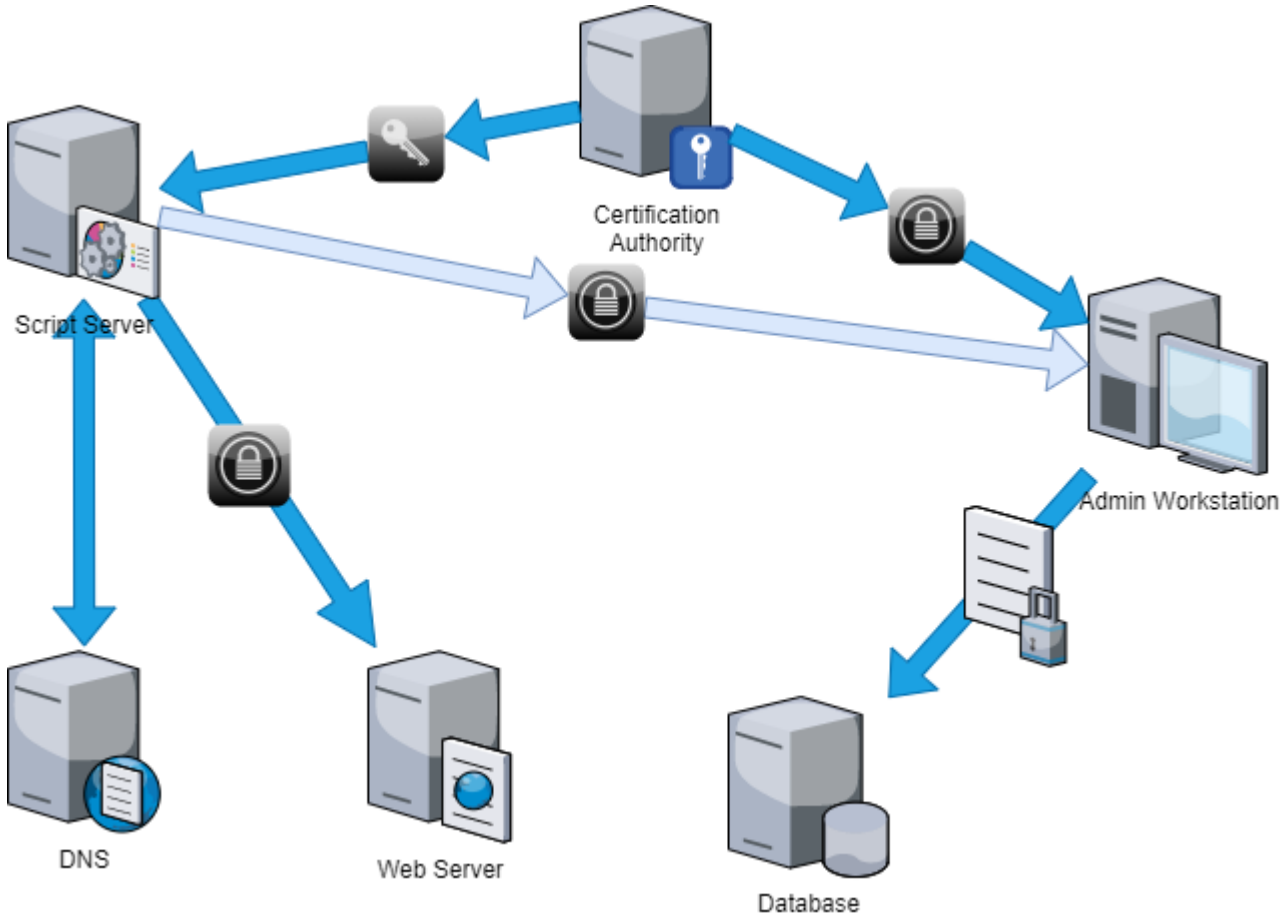
THE PLAN



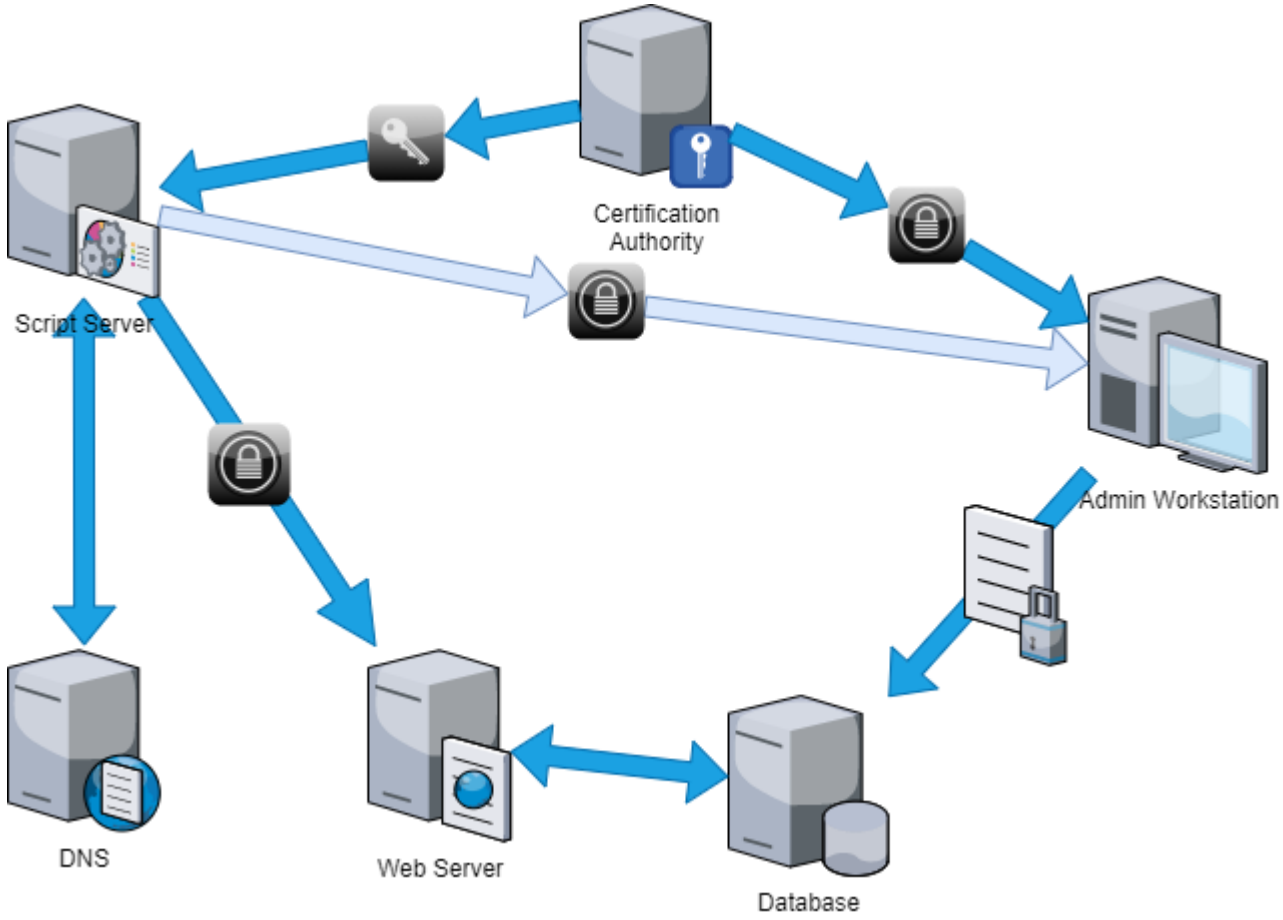
THE PLAN



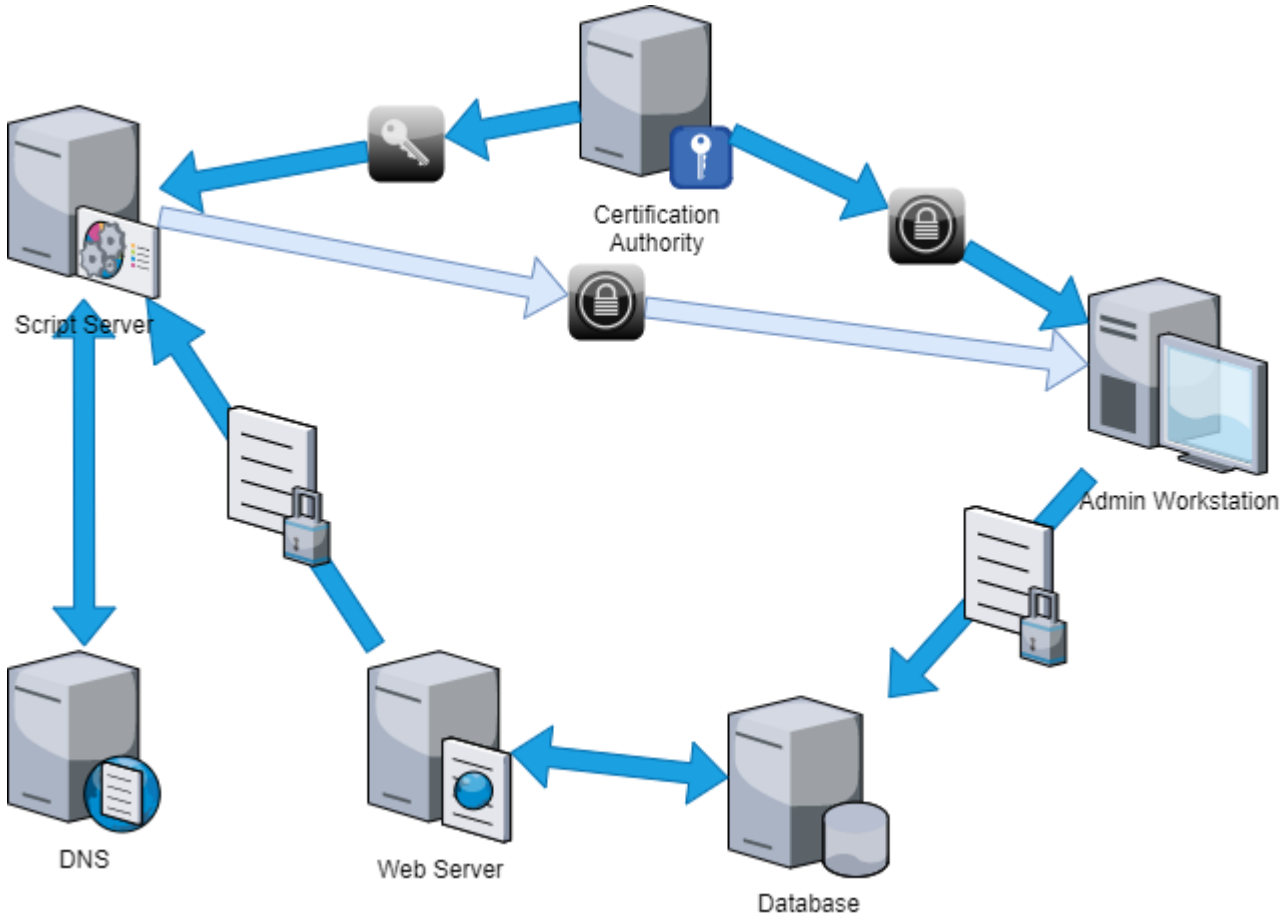
THE PLAN



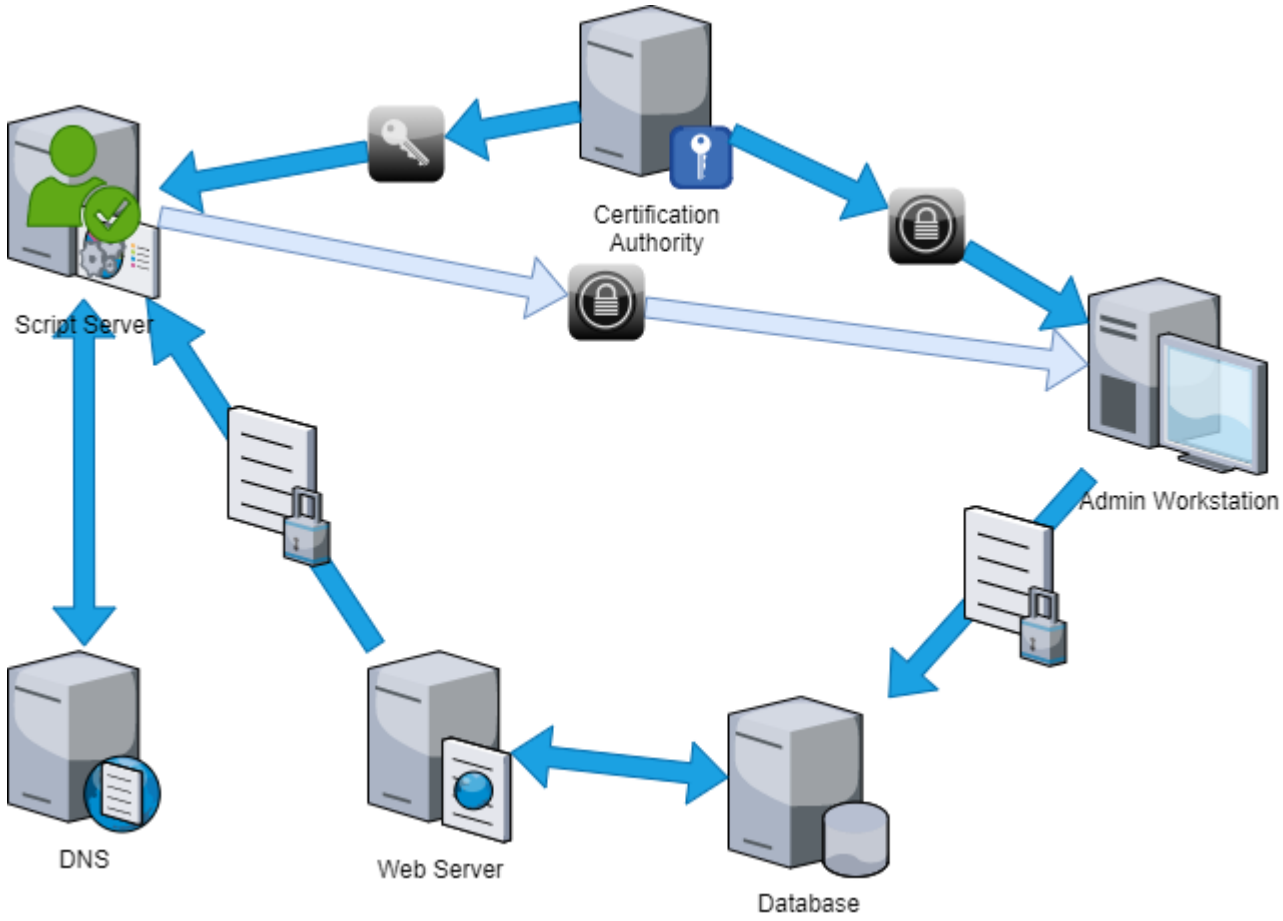
THE PLAN



THE PLAN



THE PLAN



THE SOLUTION: OVERVIEW

- **SQL database**
  - Credential admins *should* be able to write using integrated authentication
  - A read-only SQL user for web service (can be converted to Integrated if the web service runs under Domain account)
- **Web Service**
  - A single view
  - Authentication free
- **XPCMAdmin module → managing encrypted data in DB, Windows only**
  - Deployment of DB and Web Service not (yet) covered by the admin module
- **XPCMClient module → retrieving credentials from web service, cross-platform**
  - Certificate retrieval not (yet) covered by the client module

DEMO

XPCM in action

CURRENT STATE & OUTLOOK

- **PoC quality, unpublished.**
- **When all functions work and have at least a rudimentary help, I will make it 0.1 and publish to GitHub (watch my blog for announcements).**
- **When I found out how to deploy the web service with PowerShell, I will make database creation and web service deployment part of 0.5 and publish it to the Gallery.**
- **To do:**
  - Resolve-DNSName on Linux (*won‘t get it with 7.1*)
  - Xplat Admin module (*not a high priority*)
  - Some basic RBAC in Admin module
  - Optimise Web service (*and maybe port to .NET Core so can be made xplat also*)
  - Optimise decryption cert retrieval on Linux
  - Requesting and obtaining certs, if cross-platform possible

Any questions?

You know where to find me ☺

This slide deck will be published on my blog.