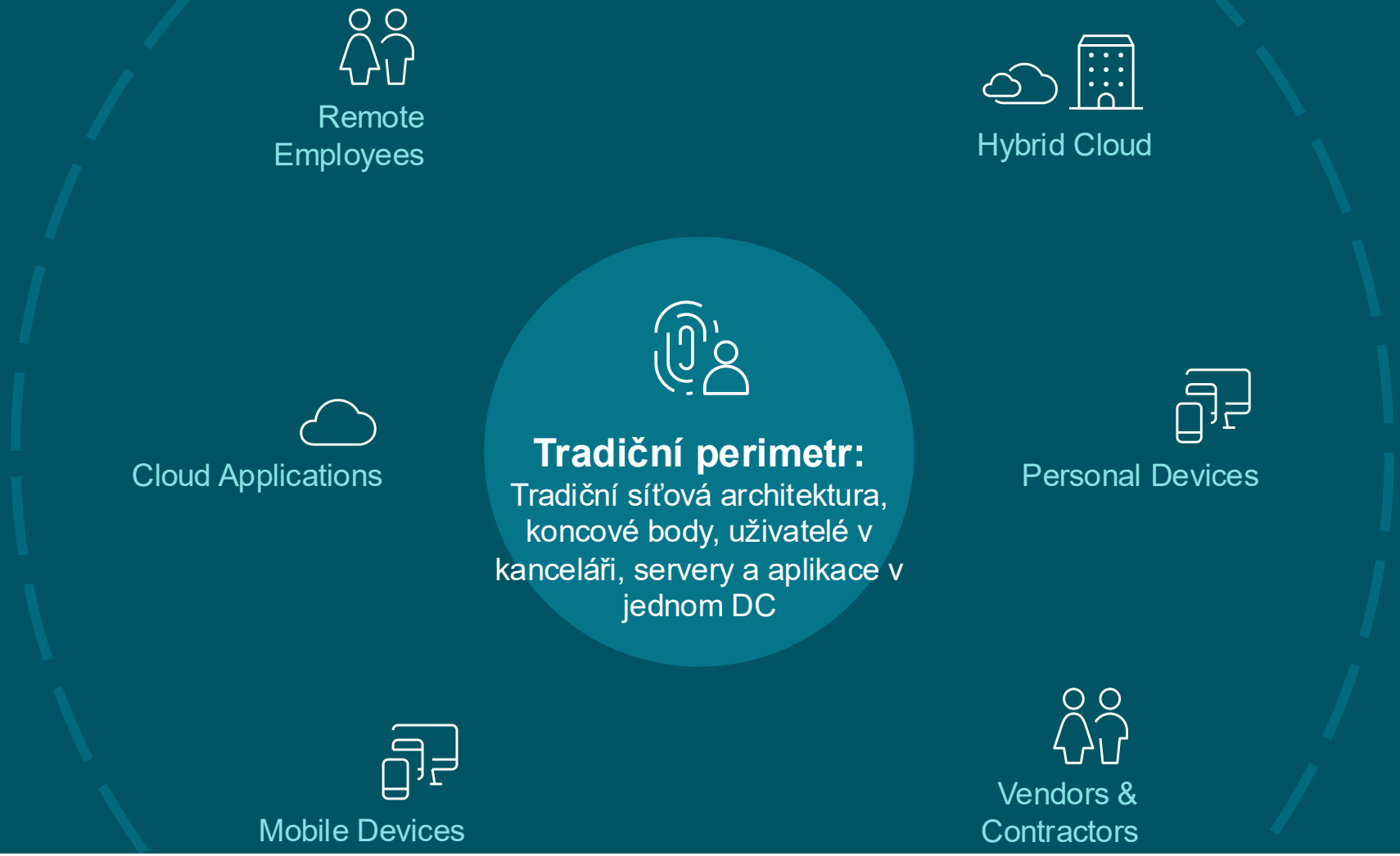

**Roman Kapitán, Tomáš Kiedroň**

21.-22. října 2021

# 17. ZÁKAZNICKÝ DEN

## Možnosti dvoufaktorové autentizace a bezpečnost na aplikační úrovni

# Proč potřebujeme Zero Trust?




Organizace potřebují nový model zabezpečení, který se účinněji přizpůsobí složitosti moderního prostředí.

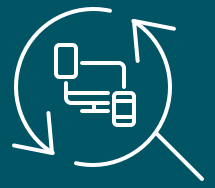


citrix

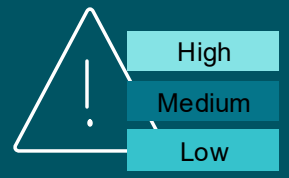
# Jak má Zero Trust fungovat?

## Nulová důvěra v organizaci jako hlavní princip

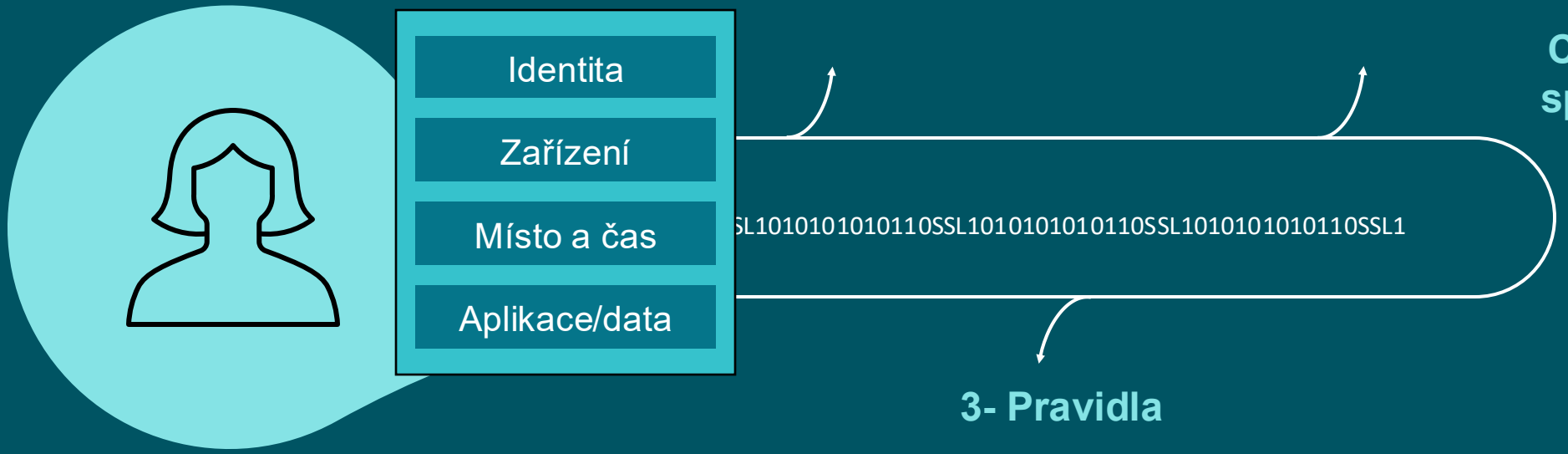
**1 - Autentikace**



**4 - Dohled**




**2 – Zhodnocení rizik**




**Centrální zobrazení, správa a vynucování opatření**

**3- Pravidla**

citrix

# Co je Zero Trust Network Access a jak se liší od VPN?

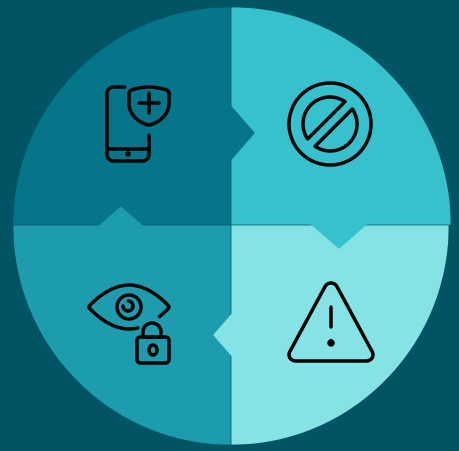
| | Rizika | Správa | Provoz a shoda |
|---|---|---|---|
| **VPN** | Odhaluje celou síť a zvyšuje pravděpodobnost útoku | Nasazení v datovém centru a obtížná údržba | Mělo by se používat pouze s firemními spravovanými zařízeními |
| | Vyžadování externí IP adresy a poskytování přístupu k uživatelským zařízením na úrovni sítě | Není dobře škálovatelné a řešení kapacitních problémů vyžaduje čas. | Přesměrování provozu přes datové centrum zpomaluje některé aplikace a působí problémy s datovou shodou. |
| **ZTNA** | Přístup zprostředkovaný na úrovni aplikace zabraňuje hrozbám na úrovni sítě<br>Přístup povolen pouze po ověření důvěryhodnosti a autorizace<br>Průběžně monitorováno a adaptivně vynucováno | Moderní cloudové služby umožňují automatické škálování, integrace | Přístup do sítě jen když je to nutné, bez přímého přístupu k datovým silům |

citrix

# Problémy, které Zero Trust a ZTNA adresuje

Ověřování a autorizace uživatelů a zařízení, integrace se stávajícími infrastrukturami.

Zabezpečený vzdálený přístup k neveřejným podnikovým aplikacím



Ochrana proti internetovým hrozbám zajišťující odstup "air gap" od firemní sítě

Průběžné monitorování, řízení a prosazování zásad informační bezpečnosti technickými prostředky.

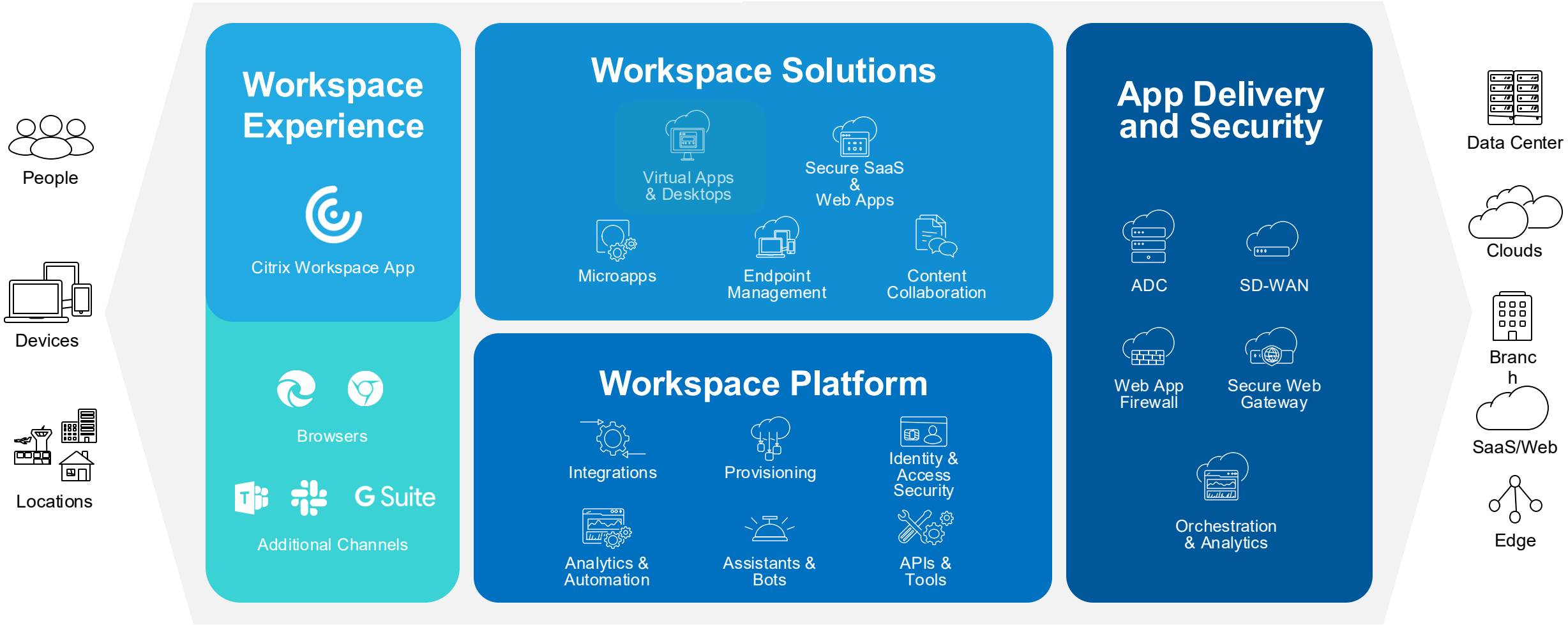
Ochrana citlivých informací

ZTNA umožňuje uživatelům přístup k neveřejným aplikacím na zařízeních BYO. IT implementuje zásady na základě polohy uživatele, stavu jeho zařízení a díky průběžnému vyhodnocování definuije další ověřovací kroky nebo ukončí přístup, pokud je riziko vysoké.

citrix

# Citrix Workspace

- platforma sjednocuje přístup uživatele k různým zdrojům
- zjednodušuje a sjednocuje správu a bezpečnost



# Workspace DEMO

citrix

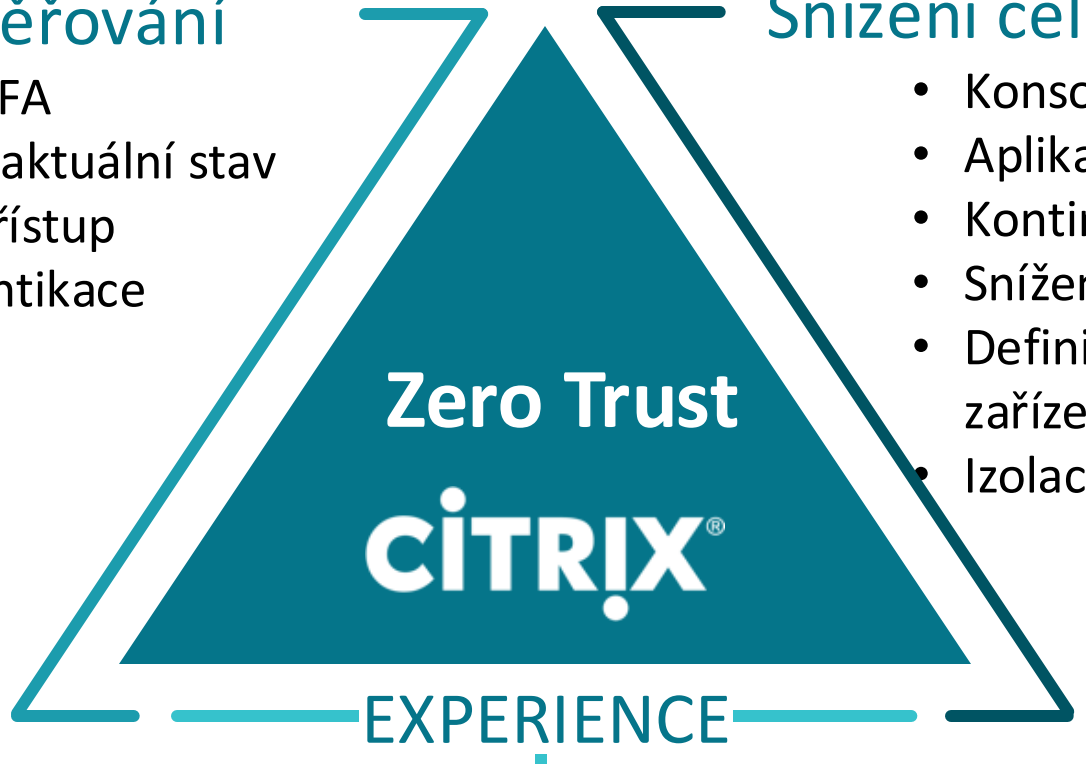
# Hlavní body Zero Trust bezpečnostní strategie podle Citrixu

## Pokročilé ověřování

- Identita and MFA
- Zařízení a jeho aktuální stav
- Kontextuální přístup
- Průbežná autentikace

## Snížení celkového rizika

- Konsolidace prostředí
- Aplikační & API bezpečnost
- Kontinuální monitoring
- Snížení komplexity IT
- Definice řešení pro nespravované zařízení a aplikace
- Izolace prohlížečů




### Uživatel:

- Neviditelnost
- Konzistence
- Jednotnost a jednoduchost

### Admin a IT organizace:

- Rychlý, intuitivní, delegovatelný dohled
- Možnosti integrace
- Úroveň centralizace
- Rychlost reakce na incidenty a změny

citrix

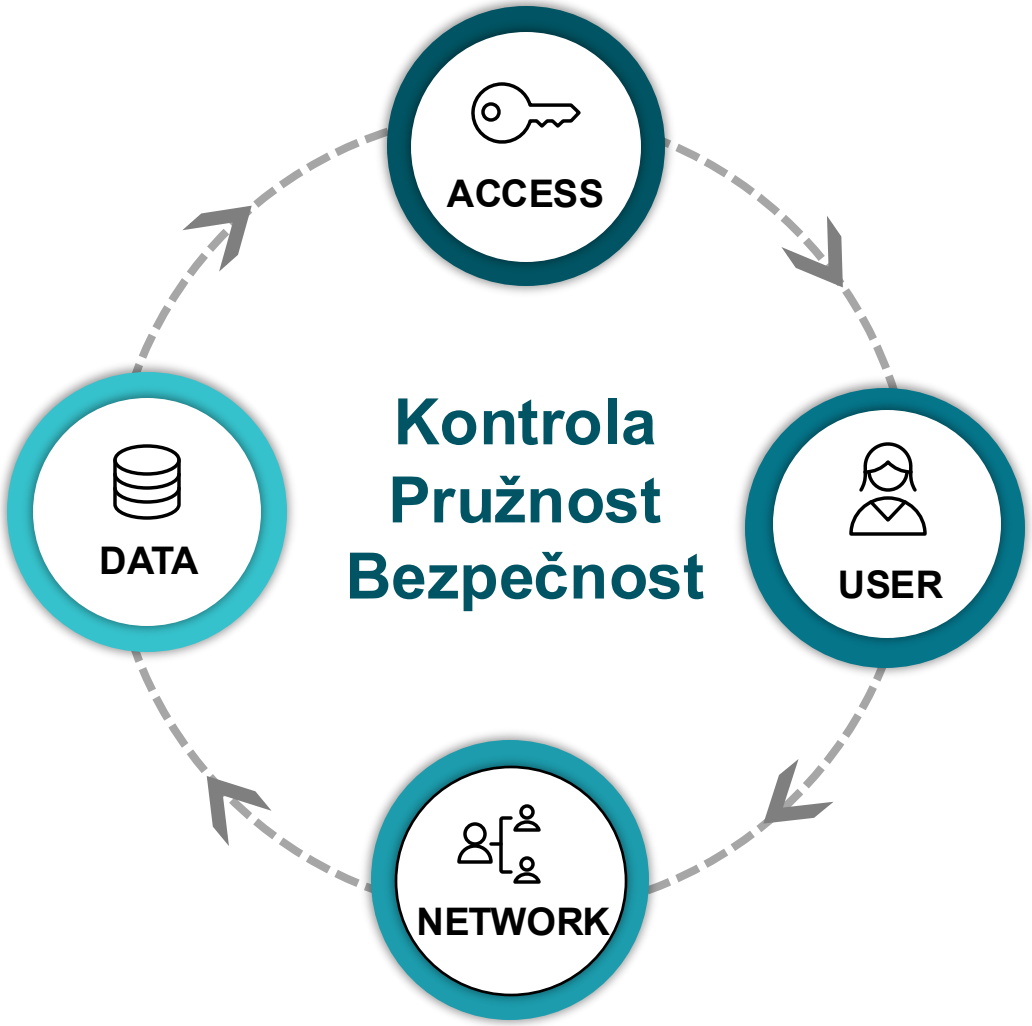
# Citrix Workspace

## Kde tedy přináší hodnotu?

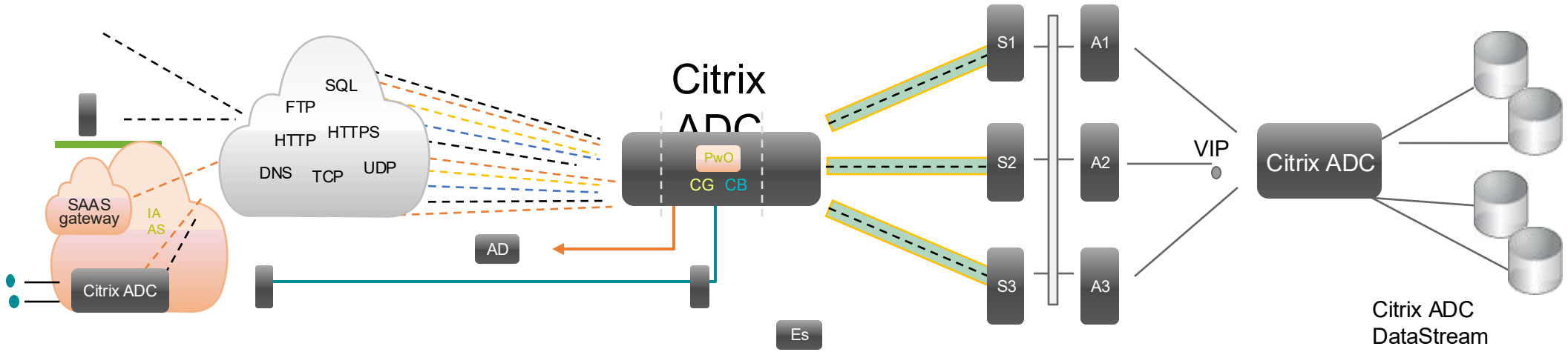
Citrix Workspace poskytuje jednotné prostředí s jediným přihlášením ke všemu potřebnému pro práci včetně přístupu ke všem aplikacím, plochám a souborům.

Citrix Workspace mění pracovní prostředí zaměstnanců tím, že organizuje, řídí a automatizuje práci, což vede k lepším obchodním výsledkům díky lepšímu zapojení zaměstnanců.

Citrix Workspace jako moderní middleware usnadňuje změny v IT aplikačních systémech, infrastruktuře a na koncových zařízeních; doplňuje prvky bezpečnostní kontroly, sjednocuje bezpečnostní pravidla a dohled nad nimi.



# Citrix ADC




Availability

- Load Balancing (SLB)
- N+1 Clustering
- L4-7 Request Switching
- Advanced Health Checks
- Content Switching
- Cache Redirection
- Global Load Balancing (GSLB)
- Dynamic Routing / PBR
- HTTP Callout
- Citrix ADC DataStream

Security

- SSL Offload
- L4-7 ACL
- Network ACLs
- DoS Protections
- Rewrite + Responder
- Rate Limiting
- SSL VPN
- AAA for App Traffic
- Application Firewall
- Citrix Gateway

Optimization

- SSL Offload
- TCP Offload
- TCP Buffering
- Surge Protection
- Compression
- Caching
- Web Logging
- HTTP 2.0
- Client Keep-Alive
- SACK/Nagles
- TCP

Management & Visibility

- CLI/GUI
- Nitro REST API
- PowerShell
- MSSCVMM/MSSCOM
- AppFlow
- Syslog
- SNMP
- AppExpert Policies

Platforms

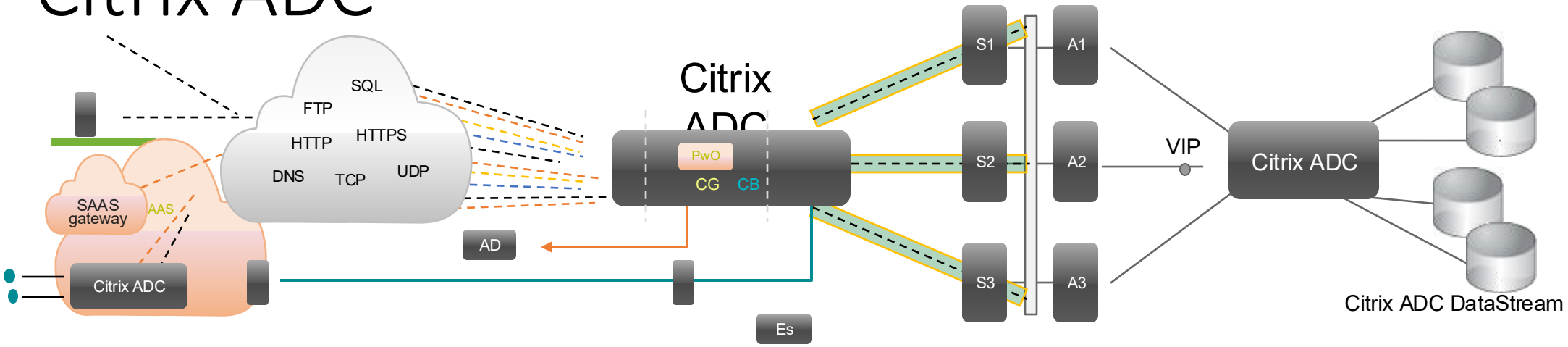
SDX
MPX
VPX
CPX
BLX

Editions

Standard, Advanced, Premium

Pay-As-You-Grow

# Citrix ADC




Availability

**Load Balancing (SLB)**

**Content Switching**

**Global Load Balancing (GSLB)**

Security

**SSL Offload**

**DoS Protections**

**AAA for App Traffic**

**Application Firewall**

**Citrix Gateway**

Optimization

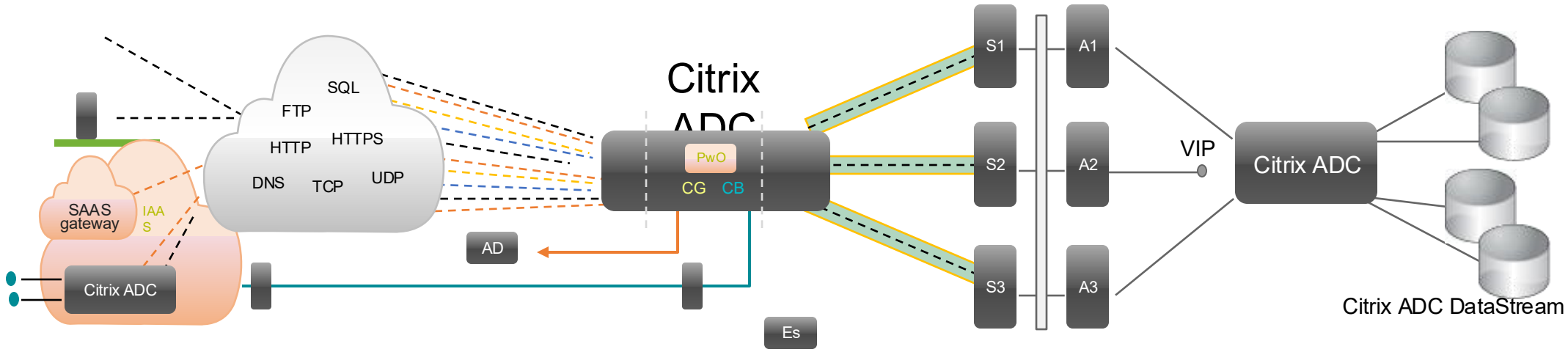
**SSL Offload**

**TCP Offload**

**TCP Buffering**

# Použití Citrix ADC

# Citrix ADC




Availability

Security

Optimization

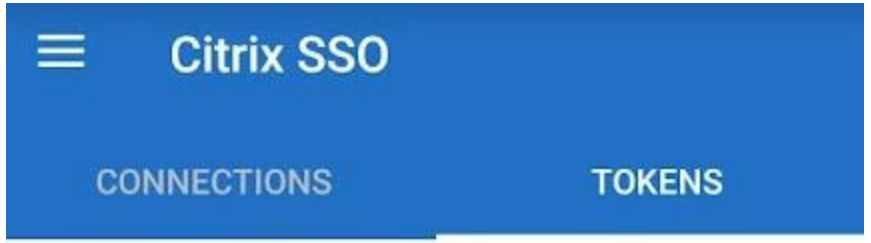
**AAA for App Traffic**

# Dvoufaktorové ověření

**Dvoufázové ověření** (**2FA**, anglicky *two-factor authentication*)

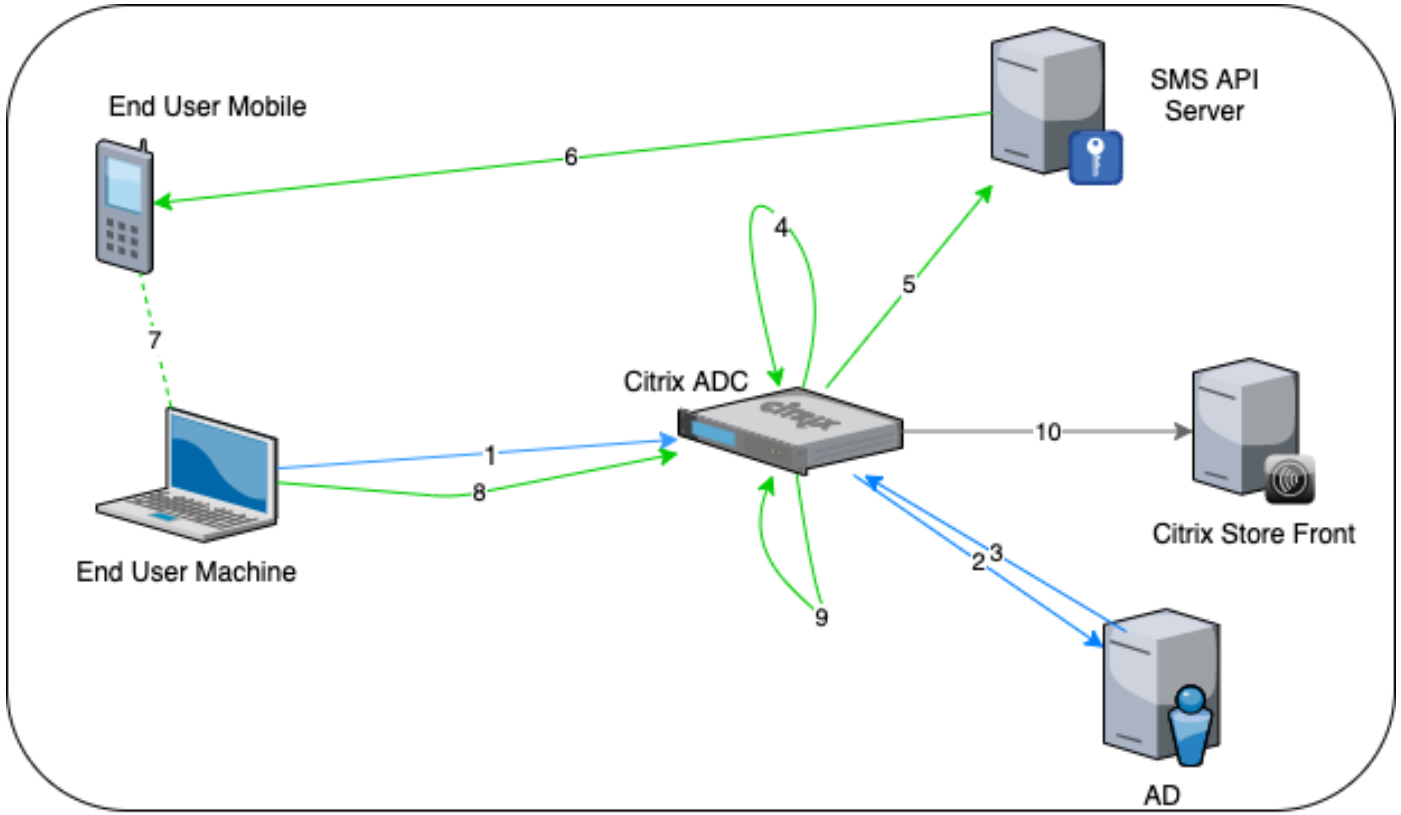
Vyžaduje od uživatele prokázání dvou faktorů (prvním je obvykle uživatelské jméno a heslo, druhým pak například PIN, otisk prstu, snímek sítnice oka, elektronický token a podobně. Dvoufázové přihlášení uživatelů podporují například Google, Facebook, Steam, internetové bankovnictví, mobilní bankovnictví, ...

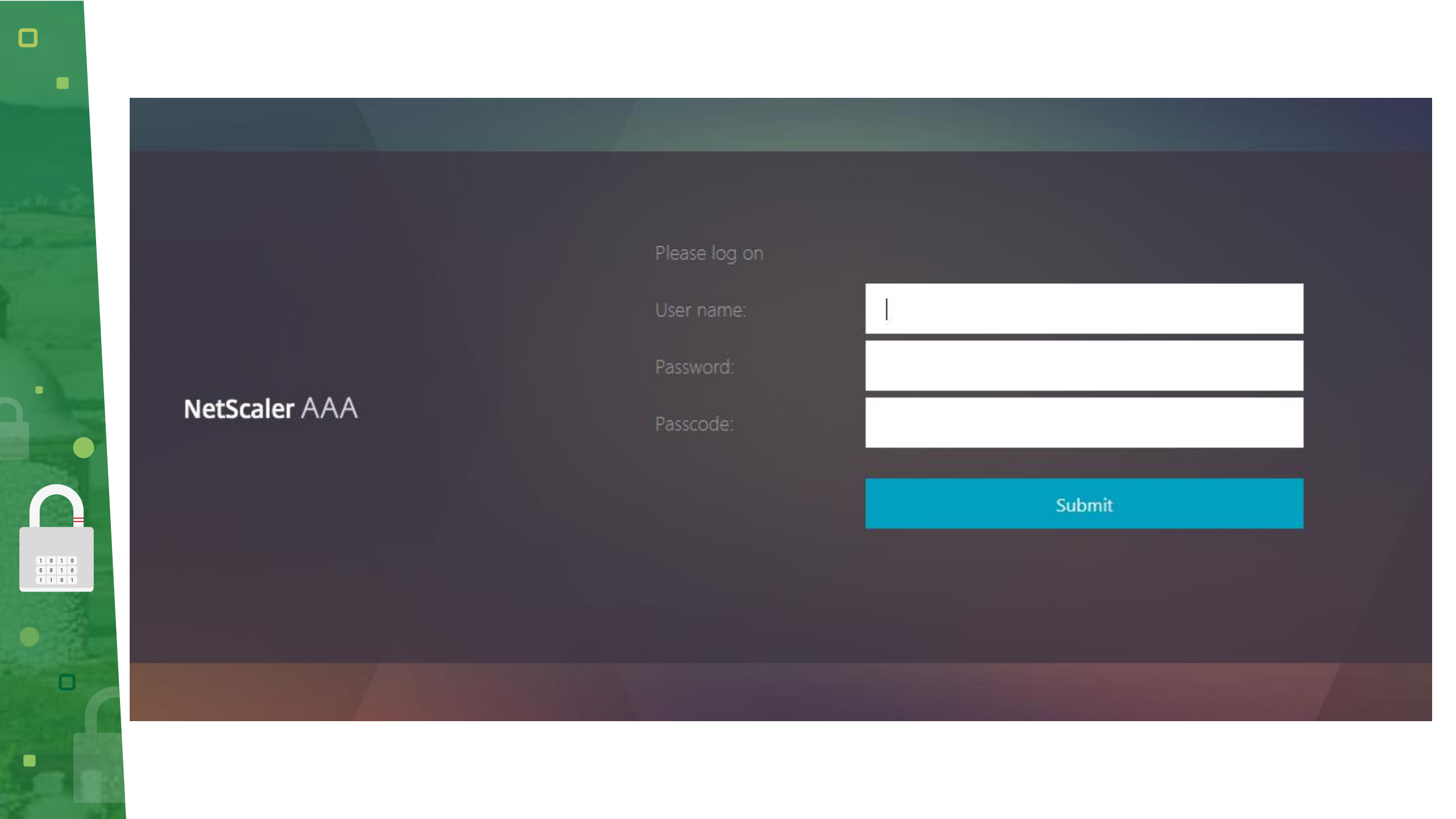
# Typy dvoufaktorového ověření

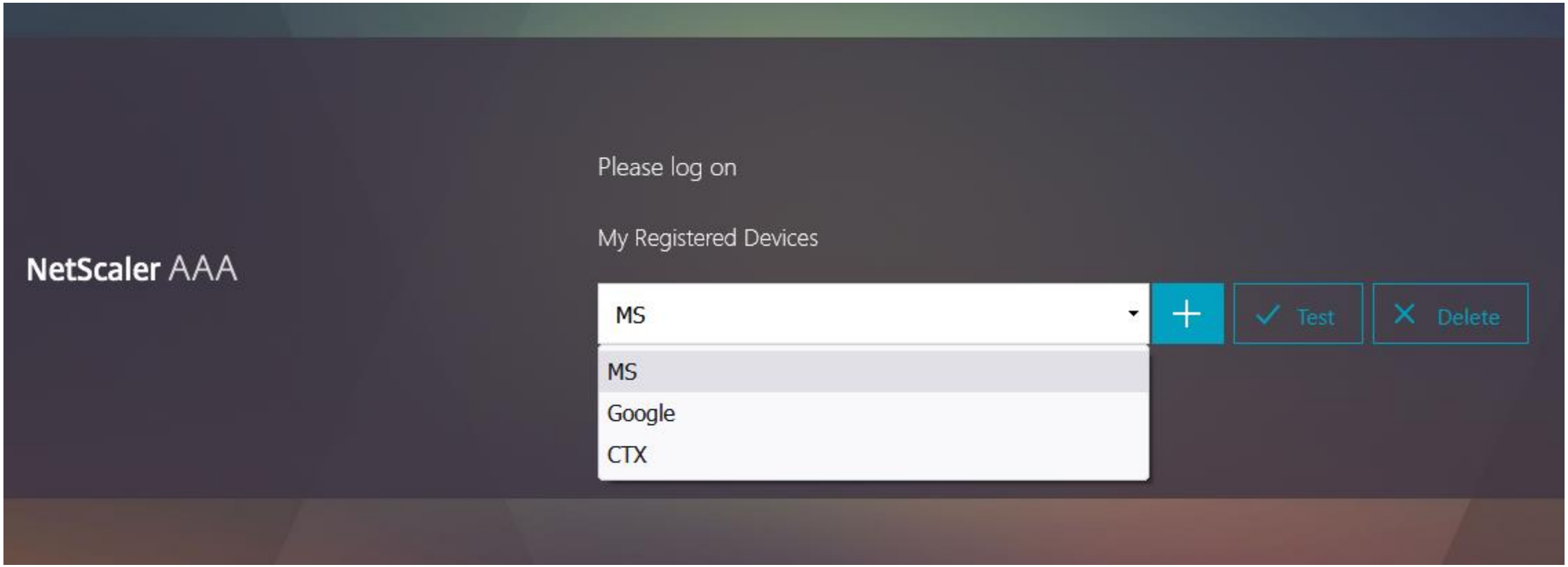



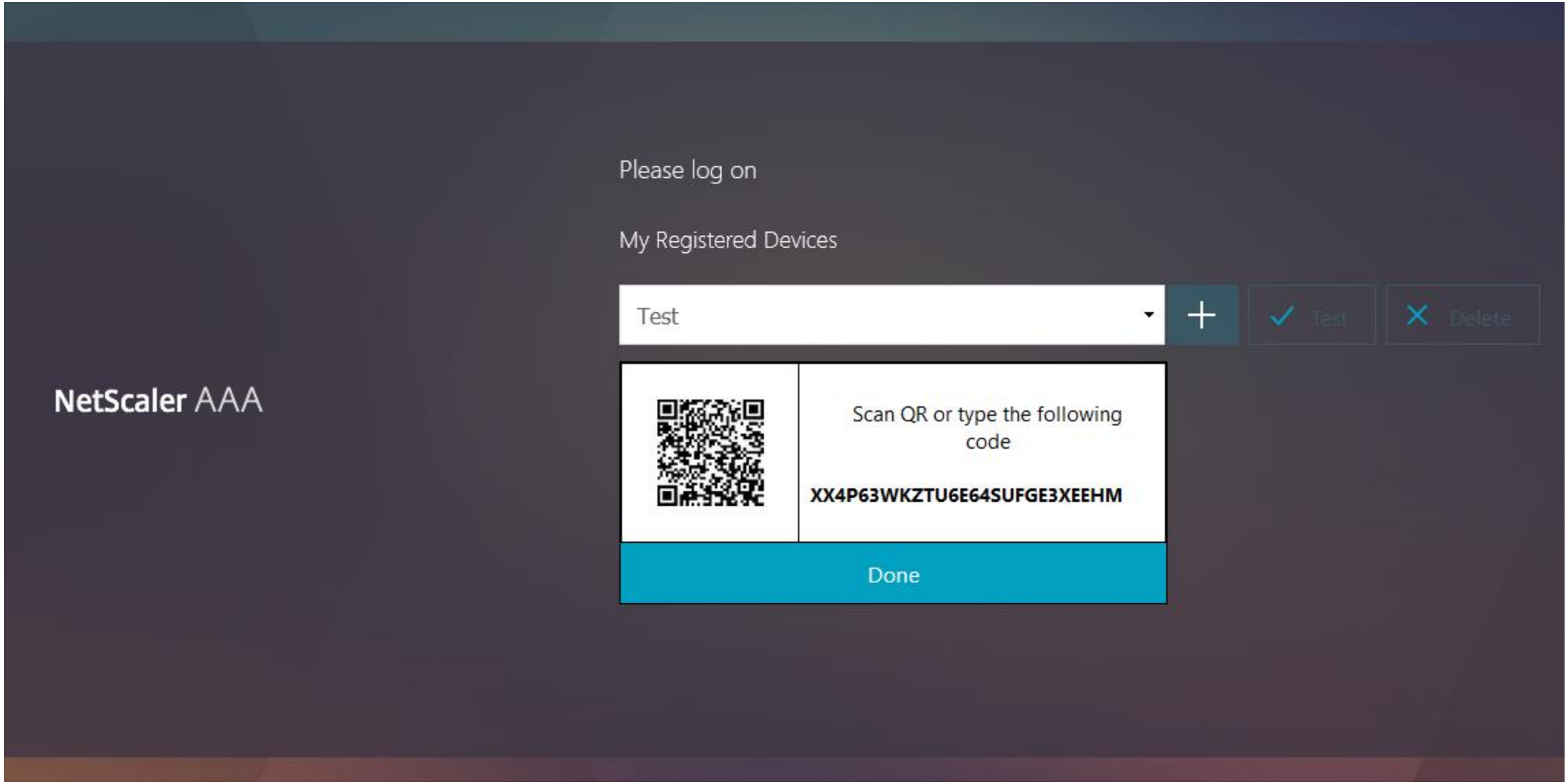


# AAA – dvoufaktorové ověřování




NetScaler AAA
Please log on
User name:
Password:
Passcode:
Submit


NetScaler AAA
Please log on
My Registered Devices
MS
Test
Delete
MS
Google
CTX


NetScaler AAA
Please log on
My Registered Devices
Test
Test
Delete
Scan QR or type the following code
XX4P63WKZTU6E64SUFGE3XEEHM
Done

# Použití Citrix ADC

21.-22. října 2021

# Děkujeme za vaši pozornost