HoloLens 2 ve firemním prostředí

Jan Grundmann

MDM Architect | Grundmann@kpcs.cz

O čem to bude

Představení

Správa

Použití

Představení

Jak HoloLens2 vypadají?

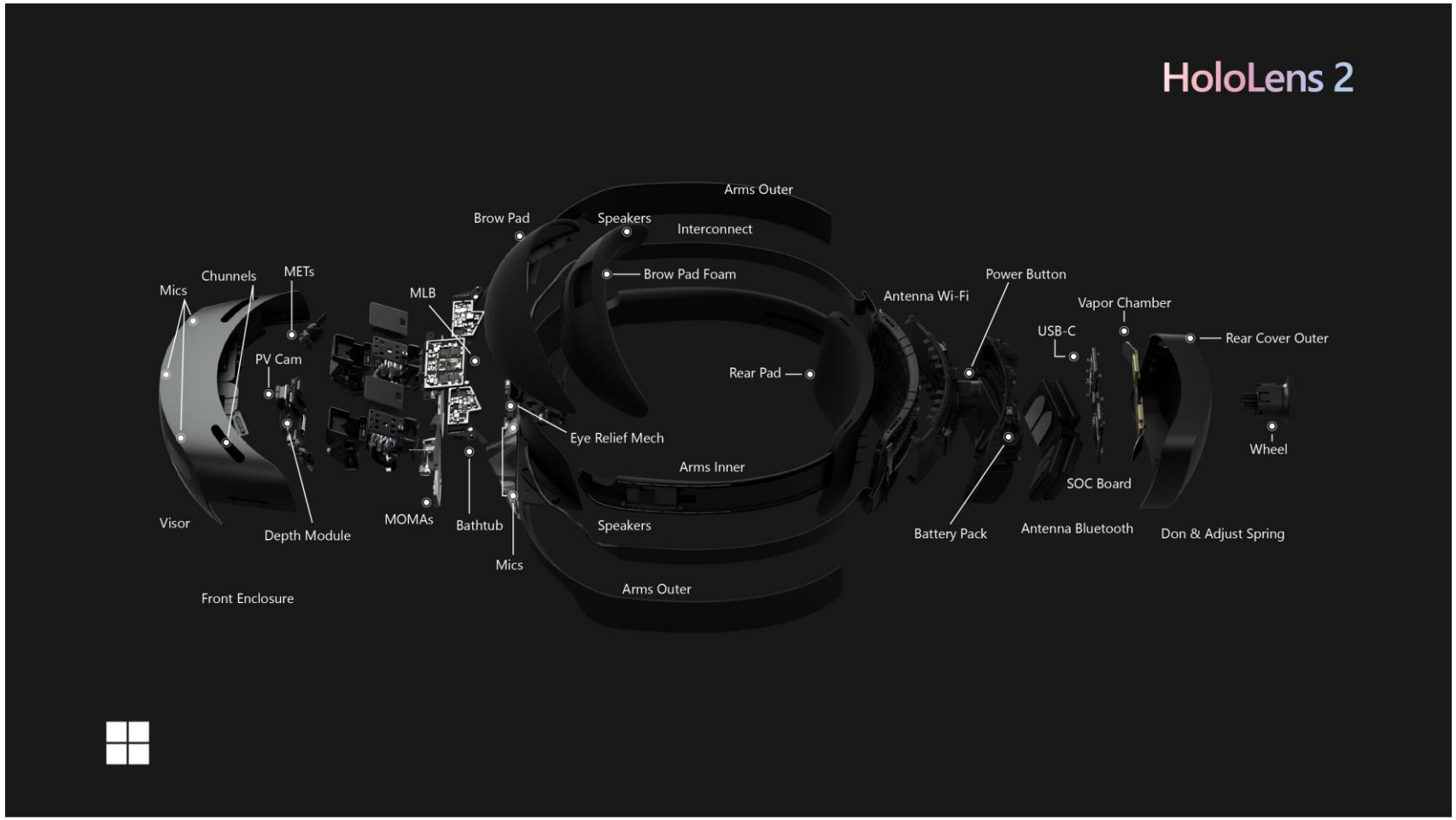
Hardware

- SoC Snapdragon 850 (ARM64)
- 4GB RAM
- 64GB UFS 2.1
- Wi-Fi 802.11ac 2x2
- Bluetooth 5.0
- USB Type-C
- 566 gramů
- Výdrž na baterii 2-3 hodiny
- Pasivní chlazení
- Nabíjení i při používání (nabíječka >15W)

Senzory a zobrazení

- 4 kamery pro snímání prostoru
- 2 infračervené kamery snímající pohyb očí
- 1-MP senzor hloubky (3D skener)
- Pohybové senzory: akcelerometr, gyroskop, magnetometr
- 8-MP fotoaparát umožňující 1080p30 video
- Zobrazení
  - Laser beam scanning – krok zpátky v kvalitě obrazu oproti HL1
  - 3:2 – 43°x29° FOV, naopak výrazné zlepšení od HL1, člověk přirozeně vidí 220°
  - 1440x936 pixelů
  - 60 FPS
  - 500 nit

Jak je to poskládané?



Síťová konektivita

- Wi-Fi
  - 2.4 i 5 GHz
  - Podpora pro nejčastější EAP metody
- Ethernet přes USB-C
- Mobilní internet přes USB-C z telefonu
- VPN
  - Built-in klient s podporou IKEv2, L2TP, PPTP
  - UWP aplikace
- Proxy
  - PAC
  - WPAD
  - Staticky server:port

Další konektivita

- Bluetooth
  - Myš a klávesnice
  - Audio výstup
- USB-C
  - Myš, klávesnice
  - Úložiště
  - Ethernet
  - 3.5mm adaptéry
  - Externí mikrofon
- Miracast

Software

- Windows Holographic OS 22H1 Build 20348
- Microsoft Edge
- Microsoft Store
- OneDrive
- 3D Viewer
- Pošta a Kalendář
- Dynamics 365 Remote assist
- Dynamics 365 Guides
- Chybí: Office, Teams a mnoho dalších

Bezpečnost

- TPM
- Bitlocker always-on
- UEFI Secure Boot
- Firewall always-on
- Žadný antivirus ani EDR by default
- Windows Defender Smart Screen – lze ovládat jen přes CSP
- Windows Defender Application Control – opět jen přes CSP
- Separace komponent OS
  - Core OS
  - OS Data
  - User data

Správa

Správa aneb „mobil s Windows“

- Moderní správa je alfa a omega
  - Čistě cloudové zařízení: AzureAD a MDM
- Enrollment
  - Interaktivní
    - OOBE
    - Nastavení
  - Automatický
    - Windows Autopilot
- Unenroll jde pouze po Enrollmentu z Nastavení lokálního nebo Microsoft účtu
  - Pokud jde o Autopilot nebo Azure AD účet - nutnost reset/reflash/wipe zařízení
- Omezené CSP třídy Windows 10
- Chybí: CMD/PowerShell, mmc, registry a další

Windows Autopilot

- Self-deploying
- Zero touch vyžaduje konektivitu přes USB-C Ethernet
  - Pokud nemá, interaktivně seznámí s ovládáním a chce připojení k Wi-Fi
- Registrace stejná jako u normálních Windows
  - Doporučeno využít Partnera, nebo Microsoft Support
  - HW hash lze získat přes offline diagnostiku a vykopírovat ze zařízení
- Tenant lockdown
  - CSP policy naváže brýle k AAD tenantu
  - Nedovolí jiný setup než Autopilot (nepovolí offline setup)
  - Zachová se i přes reset/reflash OS, zapisuje se do UEFI

Offline správa

- Windows Configuration Designer -> provisioning packages (PPKG)
- Přímo v zařízení
  - aplikace Nastavení
- Advanced Recovery Companion
  - USB do PC
  - Reset a reflash OS
- Device Portal

Identity

Lokální

- První uživatel z OOBE
  - 1:1
- Visitor/Guest
  - Vytvořen pouze přes CSP nebo PPKG

Cloudové

- Microsoft account
  - 1:1
- Azure AD uživatelé
  - 64:1
  - Odebírání ručně v Nastavení
  - První přihlášený uživatel je „Device owner“ (“admin”)
    - Výjimka u Autopilotu a bulk AAD enrollmentu

Použití typů účtů

- Lokální
  - Vytvořen v OOBE
  - Nelze přidat dalšího uživatele
- Microsoft Account
  - Přihlášen v OOBE
  - Nelze přidat dalšího uživatele
- Azure AD
  - Účet z tenantu organizace použit v OOBE
  - Zařízení prošlo Autopilotem
  - Dovoluje přihlášení pouze Azure AD účtům ze stejného tenantu

Pro přechod mezi typy účtů je třeba reset/reflash/wipe OS

Autentizace

Účet\Metoda	Heslo	Web	PIN	FIDO2	Iris biometrie	Auto-logon	Authenticator (password-less)
Azure AD	Ne	Ano	Ano	Ano	Ano	Ano	Ano
Microsoft	Ano	Ne	Ano	Ne	Ano	Ano	Ne
Lokální	Ano	Ne	Ne	Ne	Ne	Ne	Ne

Aplikace

- ARM64 UWP
- Sdílené pro všechny uživatele, uživatel má svá appdata
- 2D nebo Holografické
- Původ
  - Předinstalované
  - Microsoft Store/Store for Business
  - MDM (available přes Company Portal)
  - Provisioning package
  - App Installer
  - Developer mode a „Windows Device Portal“

Device lockdown

- Omezení Nastavení
  - PageVisibilityList – specifikace, co je viditelné uživateli
- Kiosk mode
  - Single app – bez Start menu, automatický start vybrané aplikace
  - Multi app – Start menu obsahuje pouze specifikované aplikace
  - Scoping na konkrétní uživatele, AAD skupinu nebo Device Owners
- WDAC
  - Vytváření na PC přes PowerShell
  - Informace o aplikacích na HoloLens lze získat jen z Device Portal
  - Nasazení přes CSP
  - Lze nasadit více policy

Aktualizace OS

- Následuje praktiky standardních Windows 10
  - 2x ročně velký release
  - Měsíční aktualizace oprav a bezpečnostní záplaty
- Dostupné v Nastavení
- Windows Update for Business: „Windows 10 update ring“
- Lze specifikovat WSUS server
- MDM nastavení
  - Aktivní hodiny, restart chování
- Delivery Optimization Preview
  - Jen HTTP nebo Microsoft Connected Cache host
  - Pouze pro OS
  - Nelze při použití WSUS

Poslední release 22H1

- Vyšel v půlce dubna
- Build 20348.1513 – stejný major jako 21H1 a 21H2 – žádné velké věci
- Color-blind mode s různými filtry
- Spouštění druhotných aplikací v Single app kiosk módu
- Moving platform mode
  - Používání hologramů pokud se konstantně pohybuji
  - např. loď, letadlo, auto

Insider Preview

- Build 22621 (22H2?)
- Autopilot vylepšení UX
- User profile cleanup (AccountManagement CSP) – rozšířené možnosti
- Podpora pro Wi-Fi captive portal na přihlašovací obrazovce
- StorageSense (Policy CSP – Storage) – úplně nově

Licence

- Enterpise Mobility + Security (Azure AD premium pro MDM Autoenrollment)
- Dynamics 365 Remote Assist
- Dynamics 365 Guides

Device portal

- Web server pro remote monitoring a management Windows zařízení
- Umožňuje např:
  - Přístup k filesystému
  - Správu Wi-Fi sítí
  - Logování ETW
  - Zapnout Kiosk mód
  - Spravovat aplikace
  - Monitorovat výkon
  - Monitorovat veškeré běžící procesy
  - Debug 3D a AR funkcí

Použití

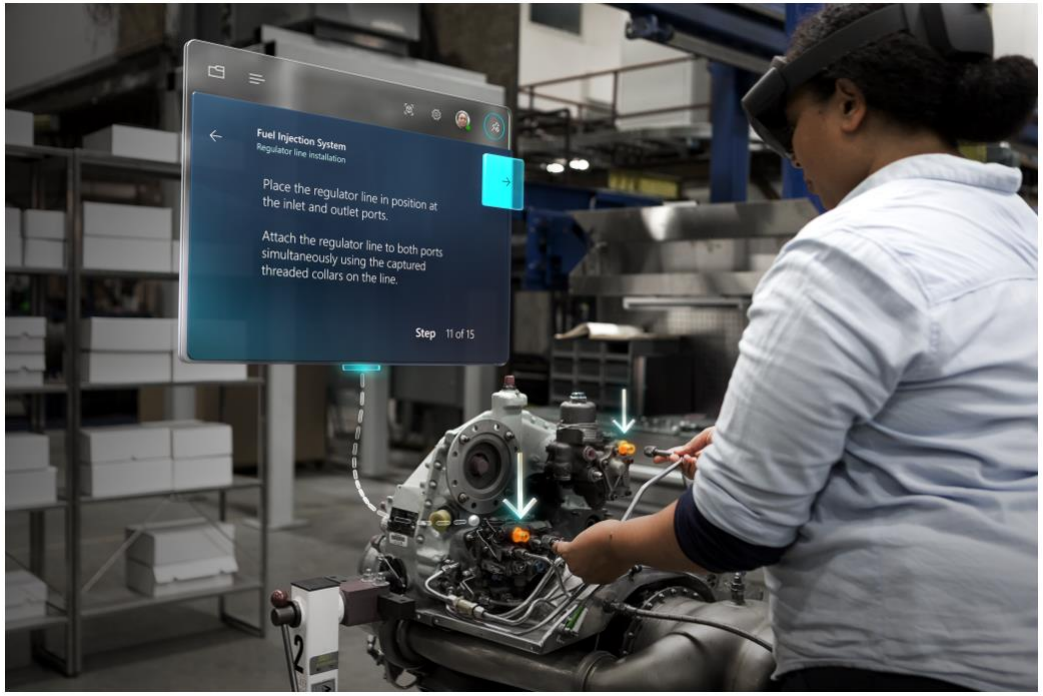
Možnosti využití

- D365 Remote Assist
  - Teams hovor obohacený o interakci nad obrazem z brýlí
- D365 Guides
  - Předpřipravené interaktivní návody interagující s rozšířenou realitou
- Microsoft Mesh
  - Platforma pro komunikaci a spolupráci v AR a VR
- Vlastní AR aplikace
  - Podpora v Unity framework – MRTK v3 (Microsoft Mixed Reality Toolkit)

Remote assist

- Kolaborace v AR
- 1:1 hovor i plánovaný meeting
- Lze volat i mezi brýlemi
- Nativní podpora v Teams desktopovém a mobilním klientovi
- Řízeno přes Teams policies – external access
- Pro plánovaný meeting je třeba Exchange online licence
- Nahrávání je závislé na zařízeních, která se připojují

Guides



- Interaktivní průvodce procesem
- Role Autor a Operator
- Autor tvoří návody v počítače
- Operator je pak následuje v brýlích
- Kotvení reality s virtuálním návodem
  - Azure Object Anchors – služba s cloudovým rozpoznáváním na základě 3D modelů
  - QR Code – umístěný v realitě – nejpřesnější
  - Circular code – podobný jako QR code
  - Holographic – lokální rozeznávání na základě oskenovaného 3D modelu

Typová prostředí k nasazení

- Cloudové
  - Aplikuje se moderní management
- Hybridní
  - Mobilní zařízení v cloudu, Windows v hybridu. HoloLens mají od každého něco
  - Nutné upravit stávající konfiguraci a implementovat nová řešení
- On-premises
  - Zavést moderní management nebo zůstat Offline
- Offline
  - Zabezpečené provozy bez přístupu k internetu
  - Vyžadují více či méně kompletní Offline scénáře
  - Typicky „ruční správa“, WCD umožňuje jednou vytvořit a pak kopírovat

Typová prostředí k nasazení 2

- Armádní?

Varianty sdílení a jejich specifika

- Personální zařízení
  - „bezproblémové“
- Týmové zařízení
  - Osobní znalost a kontakty v týmu
  - Záleží na velikosti týmu
- Sdílené zařízení
  - Jednotliví uživatelé se neznají
  - Nevíme kolik lidí zařízení použije

Výzvy při nasazení

- HL2 se používá v odlišném (zabezpečenějším) prostředí, než který používají jejich uživatelé k běžné práci
- Uživatelé s dioptrickými brýlemi – lze používat, ale hůře sedí na hlavě
- Kalibrace podle očí
  - Spouští automaticky pokud HL2 nasadí na hlavu někdo jiný (i u sdíleného účtu)
  - Možnost ručně vyvolat v nastavení
- First sign-in experience
  - U sdíleného účtu po prvním přihlášení už není, uživatel musí spustit průvodce
  - U osobního účtu, pokud dojde ke promazání, může naopak zdržovat zkušeného uživatele
- Nabíjení a aplikace aktualizací
- Hygiena - čištění

Subjektivní zkušenosti

- Kvalita obrazu
  - FOV
  - Rozlišení
  - Barevná přesnost
  - Kontrast
- Ovladatelnost
  - Gesta vs hlas