Příloha č. 1 – Specifikace a rozsah předmětu plnění

1. Předmět zakázky

Předmětem zakázky je vytvoření mobilní aplikace „UK klíč“, která bude podporovat dvoufaktorovou autentizaci (dále jen „2FA“) při přihlašování do aplikací Univerzity Karlovy.

http://cuni.cz/http://ldap.cuni.cz/U mobilní aplikace bude probíhat ověřování uživatele buď pomocí PINu, nebo interním mobilním ověření ID integrovaném v telefonu (FaceID, otisk prstu, …).

Pro 2FA bude využit standard TOTP, který je využíván například v prostředí aplikací pro autentizaci od společností Microsoft a Google. Dle standardu TOTP bude časově omezený, 6-ti místný kód vygenerován uživateli aplikací UK klíč. Stejný kód může být uživateli vygenerován mobilními aplikacemi pro autentizaci společností Microsoft nebo Google. Aplikace UK klíč bude navíc schopna zaslat vygenerovaný klíč k ověření autentizační službou na pozadí, aniž by jej uživatel musel ručně opisovat do přihlašovací stránky (stále ale musí zůstat možnost zobrazit vygenerovaný klíč uživateli, tak, jako to implementují ostatní aplikace).

2. Technologické požadavky poptávaného řešení

- Backend část bude implementována s využitím jedné z následujících vývojových platforem:
  - C# + ASP .NET Core,
  - TypeScript + Next.js/Nest.js,
  - PHP (výhradně s využitím objektů).
- Frontend část (mobilní aplikace pro platformy iOS a Android) bude implementována s využitím těchto vývojových platforem:
  - Swift pro platformu iOS,
  - Kotlin pro platformu Android.
- Mobilní aplikace musí stoprocentně fungovat v operačním systému iOS minimálně od verze 15.0 a v operačním systému Android minimálně od verze 7.0.

3. Požadavky na poptávané řešení

3.1 Požadavky na kapacitu a rychlost odbavení požadavků v procesu 2FA

Počty přihlášení do webového rozhraní (počty logů) jsou vedeny v následující tabulce:

období	**Počet přihlášení za období**
16.9. – 30.9.2021	754.940
říjen 2021	1,313.437
listopad 2021	752.565
prosinec 2021	774.854
leden 2022	1,545.185
únor 2022	1,467.579
březen 2022	710.612
duben 2022	706.244
květen 2022	1,205.987
červen 2022	999.349
červenec 2022	295.048

srpen 2022	397.504
1.9. – 16.9.2022	529.896
celkem za období	**11,453.200**

zdroj: SIS – podklady poskytl Petr Mikeš, vedoucí oddělení vývoje SIS ÚVT UK

Počty přihlášení do webového rozhraní SIS (počty logů) v 5-ti vybraných dnech s nejvyšším počtem přihlášení za předchozích 12 měsíců:

datum	počet přihlášení za den
4.2.2022	113.143
1.2.2022	107.849
4.10.2022	106.646
5.10.2022	98.515
7.2.2022	98.468

zdroj: SIS – podklady poskytl Petr Mikeš, vedoucí oddělení vývoje SIS ÚVT UK

Počty přihlášení do webového rozhraní SIS (počty logů) v 5-ti vybraných minutách s nejvyšším počtem přihlášení za předchozích 12 měsíců:

Datum – čas (minuta)	počet přihlášení za minutu
4.2.2022 – 14:58	1.736
4.2.2022 – 14:52	1.514
4.2.2022 – 15:00	1.505
4.2.2022 – 14:56	1.439
4.2.2022 – 14:48	1.420

zdroj: SIS – podklady poskytl Petr Mikeš, vedoucí oddělení vývoje SIS ÚVT UK

Je patrné, že požadavky na odbavení prostřednictvím navrženého kanálu pro 2FA musí garantovat:

- propustnost na úrovni alespoň 12 mil. / rok,
- propustnost na úrovni alespoň 120.000 / den,
- propustnost na úrovni alespoň 1.800 / minutu.

Tyto požadavky na počty odbavení musí naplňovat všechny komponenty SW architektury, ze kterých se navržené řešení skládá. Dále platí, že odbavení jednotlivých požadavků je nutné realizovat do 30 vteřin. Pokud bude tento interval překročen, 6-ti místný kód (způsob jeho generování je popsán níže), pozbyde platnosti a proces 2FA bude třeba opakovat, případně dokončit alternativním, nikoliv uživatelsky příjemným způsobem.

3.2 Požadavky na technologii pro 2FA

Pro 2FA bude využit standard TOTP pro generování časově omezených kódů (Time-based one-time password), který je využíván například v prostředí aplikací pro autentizaci od společností Microsoft a Google.

Navržené řešení akceptuje původní návrh oddělení infrastruktury serverů a úložišť ÚVT UK, na využití standardu TOTP a použití mobilní aplikace „UK klíč“ jej rozšiřuje o následující výhody:

- není nutné přepisování 6-ti místného bezpečnostního kódu do prostředí webového rozhraní při každém přihlášení uživatele,

- pro rychlé ověření uživatele v mobilní aplikaci bude využito moderních biometrických funkcí – otisk palce, snímek obličeje (případně jiného způsobu, kterým se uživatel přihlašuje do mobilního telefonu na úrovni OS iOS a Android)

3.3 Spárování uživatele s mobilním zařízením a přenesení privátního kódu do mobilní aplikace

Před prvním přihlášením uživatele je nutné spárovat uživatele a mobilní zařízení – mobilního telefonu, aby mohly být uživateli doručovány push notifikace. Pokud bude uživatel registrován na více zařízeních, bude dostávat push notifikace na všechna registrovaná zařízení. Dále je potřeba do aplikace „UK klíč“ přenést jedinečný kód, na jehož základě je generován jednorázový 6-ti místný kód.

Pro nastavení Smart klíče UK je potřeba mít platné ověřené CAS heslo.

V portáluhttp://ldap.cuni.cz/ CAS (centrální autorizační služba) uživatel zvolí možnost přihlašování přes „UK klíč“, kde mu bude následně zobrazen jedinečný QR kód. QR kód bude načten do mobilní aplikace přes fotoaparát a informace v něm obsažená bude přenesena do mobilní aplikace. (Alternativně bude možné zadat kód ručně). Tím proběhne jedinečné ověření mobilní aplikace uživatele v mobilním telefonu. V databázi CAS se zaznamená jedinečné ID mobilní aplikace a volba uživatele přes „UK klíč“.

Jako alternativu k manuálnímu postupu, je možné využít přihlášení uživatele do mobilní aplikace „UK klíč“. Při přihlášení uživatele do mobilní aplikace, bude voláním API zajištěno přenesení kódu do mobilní aplikace a jedinečné ověření mobilní aplikace uživatele v mobilním telefonu. Dále bude provedeno zaznamenání jedinečného ID mobilní aplikace a volba uživatele přes „UK klíč“ do databáze LDAPu. Volání bude provedeno na pozadí, bez nutnosti zásahu uživatele. Uživatel by tak nemusel scanovat QR, jak je uvedeno v předchozím postupu.

Po spárování uživatele s mobilním zařízením a přenesení privátního kódu do mobilní aplikace již nebude nutné, aby se uživatel při každé 2FA do mobilní aplikace přihlašoval. Bude dostatečné, pokud se ověří biometrických nebo jiným způsobem na úrovni mobilního zařízení, resp. operačního systému.

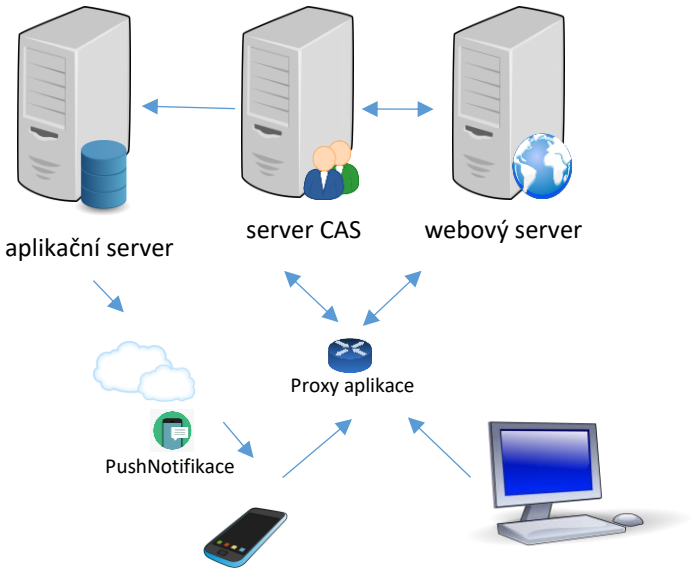
3.4 Popis procesu 2FA

Součástí řešení bude vytvoření vlastní komponenty pro zasílání push notifikací – aplikační server (nepřipouští se jakékoliv řešení třetí strany), který bude poskytovat požadavky na rychlost a kapacitu uvedené v kapitole 3.1.

Požadovaný proces 2FA bude probíhat takto:

1. Uživatel webové aplikace uvede při přihlášení do webového rozhraní CAS svoje uživatelské jméno a heslo.
2. Následně se uživateli zobrazí rovněž požadavek na použití 2FA – tedy stránka, na které si bude moci vybrat z možností, jak 2FA provést. Jednou z možností bude mobilní aplikace „UK klíč“. CAS odešle požadavek na dvoufázové ověření uživatele do aplikačního serveru, který bude součástí implementace. Požadavek bude obsahovat informace o zařízení, na které má být notifikace doručena a URL adresu, na kterou bude z mobilního zařízení odeslán generovaný 6-ti místný kód TOTP. URL adresa může obsahovat parametry pro zpětné spárování požadavku na ověření uživatele.
3. Aplikační server připraví odpovídající push notifikaci, která bude odeslána na mobilní zařízení.

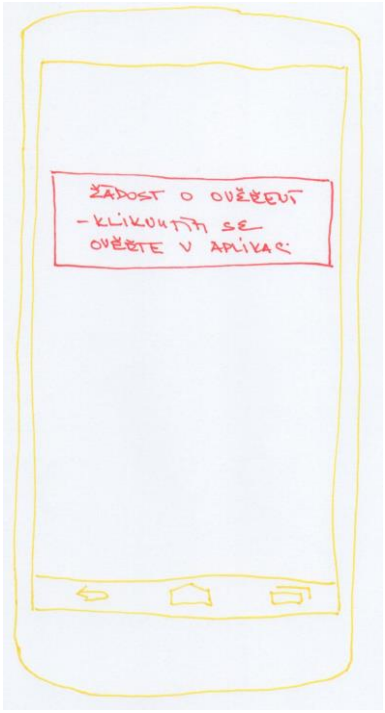
4. Uživatel na mobilním zařízení rozklikne push notifikaci, mobilní aplikace „UK klíč“ bude otevřena na stránce vyzývající k potvrzení identity. Uživateli bude zobrazena informace kdy, kam a odkud se uživatel snaží hlásit.
5. Uživatel na příslušné obrazovce potvrdí svoji identitu – PINem (záložní způsob v případě nedostupnosti následujících možností) a otiskem prstu nebo rozpoznání obličeje.
6. Mobilní aplikace vygeneruje kód TOTP a odešle jej na příslušný proxy server, který bude implementován UK. Proxy provede spárování požadavku na ověření uživatele se zaslaným kódem TOTP a zaslaný kód ověří pomocí CAS serveru. V případě shody obou kódů bude uživateli umožněn webový přístup do aplikace.



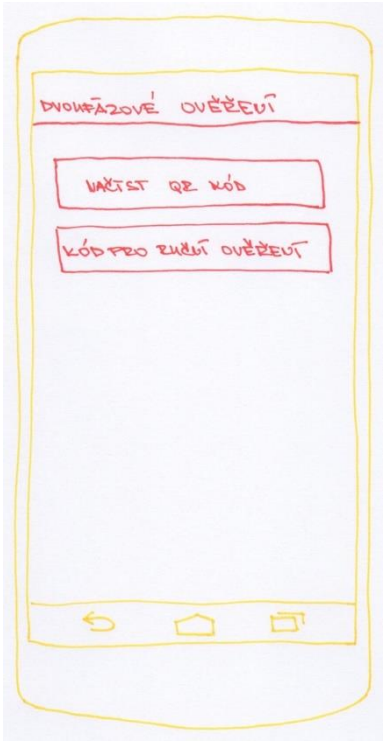
„UK klíč“ - SW architektura pro 2FA

3.5 Návrhy obrazovek mobilní aplikace

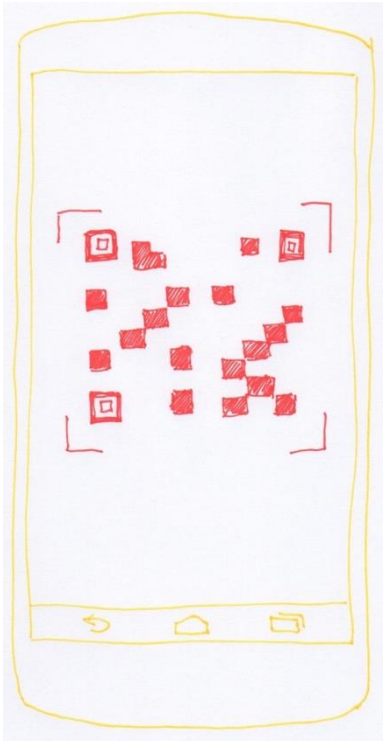
Níže uvedené návrhy jednotlivých obrazovek mobilní aplikace jsou rámcové a mohou být upraveny v předimplementační analýze.



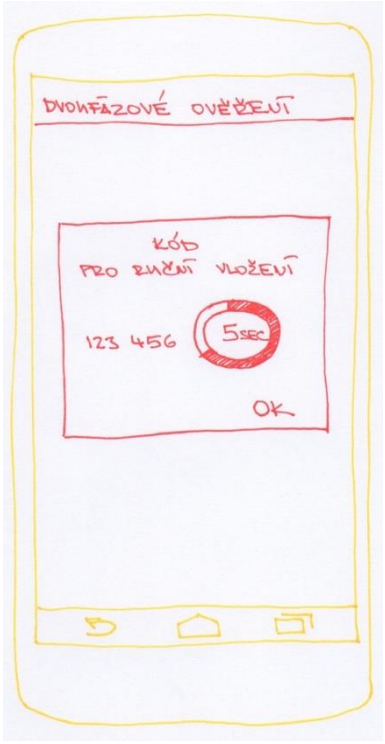
2FA – doručení notifikace do mobilní aplikace se žádostí o ověření



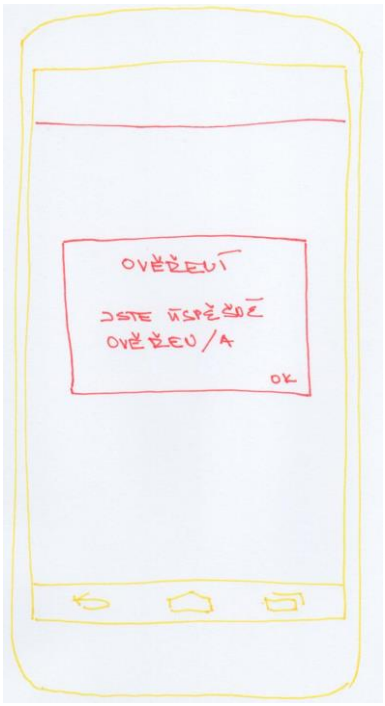
2FA – základní – vstupní – obrazovka pro ověření



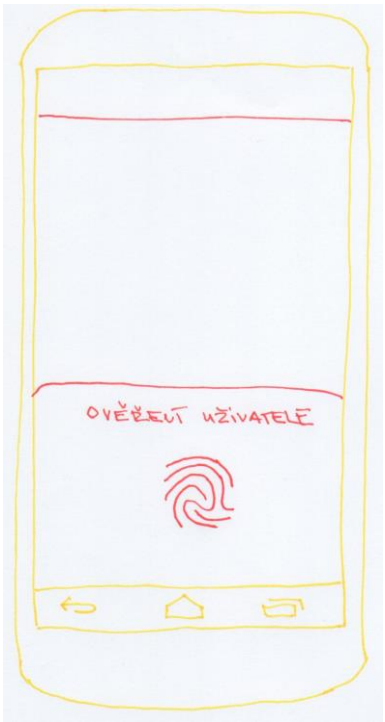
2FA – načtení QR kódu



2FA – ruční vložení 6-ti místného kódu do webového rozhraní



2FA – úspěšné ověření



2FA – systémové ověření uživatele pro přístup k aplikacím v telefonu,
tedy včetně mobilní aplikace „UK klíč“ (na úrovni OS Android nebo iOS – otisk prstu, face ID, kód)

3.6 Předimplementační analýza, případná úprava návrhu obrazovek mobilní aplikace, grafický design mobilní aplikace a návrh řešení případného výpadku služby nebo komponenty pro zasílání notifikací

Součástí zakázky bude rovněž detailní předimplementační analýza, návrh všech obrazovek mobilní aplikace ve formě wireframes, návrh grafického designu mobilní aplikace a návrh výpadku služby nebo komponenty pro zasílání notifikací.

Předimplementační analýzu provede dodavatel společně se zástupci Univerzity Karlovy, jejím výstupem bude dokument, který detailně popíše implementaci projektu. Součástí předimplementační analýzy bude rovněž návrh všech obrazovek mobilní aplikace ve formě wireframes a jejich řazení („flow“ mobilní aplikace) a návrh grafického designu mobilní aplikace na dvou vybraných obrazovkách.

Součástí předimplementační analýzy bude rovněž návrh rozhraní pro vzájemnou komunikaci jednotlivých částí systému a také návrh případného výpadku služby nebo komponenty pro zasílání notifikací.

Dokument bude protokolárně schválen zástupci Univerzity Karlovy a bude závazný pro vlastní implementaci.

4. Servisní podpora

Po dobu platnosti smlouvy bude poskytována zadavateli odpovídající servisní podpora, která bude zahrnovat minimálně:

- garance portace implementovaných modulů na další verze operačních systémů pro platformy iOS a Android,
- technickou podporu prostřednictvím e-mailu a telefonu v pracovních dnech od 9:00 do 17:00 hod.,
- udržování kódu implementovaných modulů a garance jeho dalšího rozvoje,
- opravy případných chyb po celou dobu platnosti smlouvy,
- garance dostupnosti řešení dle požadavků na kapacitu a rychlost odbavení požadavků v procesu 2FA

5. Předání zdrojových kódů

Součástí zakázky bude předání zdrojových kódů implementovaného řešení zadavateli.

6. Dokumentace k aplikaci

Dokumentace bude obsahovat:

Struktura aplikace:

- popis jednotlivých komponent, modulů a jejich vzájemné vztahy
- popis technologií, seznam technologií použitých při vývoji aplikace a jejich účel

Funkční dokumentace:

- Seznam funkcí aplikace: popis jednotlivých funkcí včetně vstupů, výstupů a chování
- Uživatelské scénáře: příklady použití aplikace

Technická dokumentace:

- Architektura aplikace: popis architektonického designu, včetně vrstev, komponent a komunikačních mechanismů.
- Datový model: schéma dat používaných aplikací a jejich vztahy