

ISIC: Back-office Identity Management a jednotné přihlašování (SSO)

ISIC Platforma je klíčovým systémem, který stojí za globálním fungováním služeb ISIC. Prostřednictvím robustní sady API propojuje lokální vydavatele do jednotného ekosystému. Platforma zahrnuje více než deset modulárních služeb pokrývajících celý životní cyklus ISIC karet a virtuálních identit, globální databázi výhod a jejich uplatňování a mnoho dalšího. Centrem platformy je ISIC Hub – jednotné back-office rozhraní zajišťující konzistentní provoz, správu dat a dohled nad vydavateli.



Hlavní výzva

Každá vydavatelská organizace funguje jako samostatná entita, která obsluhuje své území, má vlastní uživatele i interní organizační strukturu. Zatímco některá data jsou obecně dostupná, většina informací zůstává striktně oddělena v rámci jednotlivých organizací a není přístupná ostatním vydavatelům, s výjimkou oprávněných super-administrátorů. Rozsah dostupných funkcí je navíc omezen podle typu organizace a role uživatele, aby byl důsledně dodržován princip nejnižších oprávnění.

Spolehlivě nastavovat a vynucovat pravidla přístupů a zároveň zachovat správu jednoduchou a efektivní představuje zásadní výzvu při vývoji klíčové aplikace, která pracuje s citlivými osobními údaji a tvoří jeden ze základů důvěry zákazníků i partnerů.

Spolupráce s Orchitechem nám pomohla zvládnout komplexní bezpečnostní výzvu a proměnit ji v řešení, které prostě funguje.

— Radek Klein, IT Manager, ISIC Association

Řešení

Aby bylo možné tyto nároky naplnit, platforma zahrnuje specializovanou komponentu Organization Manager, která nabízí následující funkce:

- hierarchickou **správu organizací** včetně víceúrovňových vztahů typu parent-child;
- **správu identit** - osobních (uživatelských) i neosobních (aplikačních a servisních);
- **hierarchický model rolí** umožňující jejich sdružování do organizačních rolí;
- řízení přístupů na bázi **RBAC** s granularní vazbou mezi rolmi a oprávněními;
- izolaci vlastnictví dat na principu **ABAC** s respektem k organizační hierarchii;
- centralizované **vyhodnocování oprávnění a přístupových pravidel** napříč celou strukturou;
- **self-service pro organizace**, který administrátorům umožňuje spravovat uživatele a přístupová oprávnění v rámci přidělených kompetencí (od back-office nástrojů po prodejní místa);
- **self-service pro uživatele** zahrnující změnu/reset hesla a aktualizaci osobních údajů;

- komplexní **audit a logování** včetně trasování požadavků včetně uživatelského kontextu.

Autentizace je sjednocena prostřednictvím centralizovaného řešení Single Sign-On založeného na protokolu CAS. Všechny služby tak sdílejí jednotný autentizační mechanismus, tak aby používání bylo pro uživatele co nejjednodušší.

- **800+** aktivních organizací
- **1200+** aktivních uživatelských účtů
- **600+** aktivních technických aplikačních účtů
- **80+** rolí
- **300+** oprávnění
- **35 000+** přiřazení rolí
- **stovky** integrovaných aplikací
- **~500** přihlášení denně
- **2 500 000** autentizovaných API požadavků

Řešení přirozeně zapadá do našeho každodenního provozu a dává našim týmům jistotu, že přístupy jsou řízeny jednotně, bezpečně a bez zbytečné administrativní zátěže. Díky tomu můžeme platformu dále rozvíjet a škálovat, aniž bychom museli znovu řešit samotné základy identity.

Nejvíce si vážíme dlouhodobé stability řešení a kvality spolupráce. Platforma se během let ukázala jako spolehlivá a zároveň nám umožňuje postupně reagovat na měnící se potřeby. Orchitech rozumí našim specifikům našeho globálního fungování a dodává řešení, která jsou praktická, odolná a navržena s ohledem na dlouhodobou udržitelnost.

— Radek Klein, IT Manager, ISIC Association

Přínosy

Orchitech pomohl vybudovat konfigurovatelnou a nezávislou identitní platformu navrženou přesně podle potřeb globálního distribuovaného modelu ISIC. Řešení přineslo:

- **bezproblémové řízení přístupů** plně integrované do každodenního provozu;
- **flexibilní, spolehlivou a konfigurovatelnou architekturu** odpovídající požadavkům ISIC;
- vysoce **granulární řízení přístupů**, které v plném souladu s regulatorními požadavky upravuje jak přístup k jednotlivým funkcím, tak vlastnictví dat;
- **plnou kontrolu a nezávislost** nad kritickou bezpečnostní komponentou.

Platforma je v provozu více než 15 let. Zůstává robustní, stabilní a vyžaduje pouze menší evoluční úpravy odpovídající přirozenému rozvoji ekosystému.

O klientovi

ISIC Association je nezisková členská organizace odpovědná za řízení, rozvoj a globální správu průkazu International Student Identity Card (ISIC). Sdružuje více než 130 členských organizací a spojuje je jasná mise: dělat studentský život lepším.

V současnosti ISIC působí ve 110 zemích a poskytuje služby více než 2,9 milionu studentů. Nabízí jim přístup k tisícům slev na desítkách tisíc míst po celém světě.

O Orchitech

Orchitech pomáhá organizacím řídit přístup v komplexních IT prostředích. Specializuje se na řešení na míru v oblasti Identity & Access Managementu a pokrývá celý dodavatelský cyklus – od vstupní analýzy a návrhu architektury přes implementaci a vývoj nástrojů až po dlouhodobou podporu.

Působíme na trhu přes 18 let a realizovali jsme více než 100 projektů pro 50 klientů z veřejného i soukromého sektoru. Dlouhodobá partnerství, některá přesahující 10 let, potvrzují stabilitu a spolehlivost.