



PLANI I STRATEGJIK IDENTITEK SH.A. 2026



Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", Ndërtesa 111, Hyrja 1, Tiranë, Albania

NIPT: M316130430; www.identitek.al; info@identitek.al.

PËRMBAJTJA

1. HYRJE.....	2
2. Qëllimet dhe Objektivat Kryesore	2
2.1. Garantimi i prodhimit dhe shpërndarjes së dokumenteve biometrike të sigurta	2
2.2. Përditësimi i Infrastrukturës dhe Teknologjisë & Projekti i Identitetit Dixhital	2
2.3. Rritja e cilësisë së shërbimit ndaj qytetarëve	3
3. Prioritetet Strategjike 2026–2027	3
3.1. Modernizimi i infrastrukturës dhe teknologjisë	Error! Bookmark not defined.
3.2. Menaxhimi i rrezikut dhe obsoleshencës	Error! Bookmark not defined.
3.3. Forcimi i sigurisë së informacionit	3
3.4. Certifikimet ndërkombëtare	4
4. Projekti “Identiteti Dixhital për Shtetasit Shqiptarë”	4
5. Shërbimi i Kuponit Elektronik (e-Voucher) – Konsolidimi në vitin 2026	5
6. Vijueshmëria e Shërbimit: Disaster Recovery Site (DRS) & Zero Trust	6
6.1. Disaster Recovery Site (DRS)	6
6.2 Zero Trust Infrastructure	6
7. Projekti “Flag Ship”	7
8. PËRFUNDIME	7

1. HYRJE

Ky Plan i Përgjithshëm Pune për vitin 2026 përcakton drejtimet strategjike dhe prioritetet operacionale të IdentiTek SHA, në funksion të garantimit të prodhimit dhe shpërndarjes së dokumenteve biometrike për shtetasit shqiptarë—një shërbim me rëndësi të lartë publike.

Dokumenti bazohet në:

- analizën e performancës së viteve të mëparshme;
- objektivat e strategjisë kombëtare për dixhitalizimin e shërbimeve dhe sigurinë e dokumenteve të identitetit
- kërkesat e kuadrit ligjor në fuqi (ligjet 9936/2008, 8668/2000, 8952/2002, 10296/2010);
- rekomandimet e auditimeve 2023–2024;

Planifikimi për vitin 2026 është hartuar mbi të dhëna të verifikuara, analiza financiare, tregtare dhe teknike. Gjithsesi, parashikimet mbeten të ndikuara nga faktorë të jashtëm ekonomikë, politikë apo teknologjikë. Në rast ndryshimesh të rëndësishme në mjedisin ligjor apo operativ, IdentiTek do të rishikojë planin në kohë reale.

Shoqëria synon të vazhdojë modernizimin teknologjik, rritjen e cilësisë së shërbimeve ndaj qytetarëve dhe forcimin e sigurisë së dokumenteve biometrikë. Objektivat kryesore përfshijnë zhvillimin e teknikave të avancuara të prodhimit, përmirësimin e elementeve të sigurisë për të parandaluar falsifikimet si edhe automatizimin e proceseve të përsëritshme. Adoptimi i teknologjive më të fundit dhe rritja e efikasitetit mbeten prioritetet kryesore në periudhën afatmesme.

2. Qëllimet dhe Objektivat Kryesore

2.1. Garantimi i prodhimit dhe shpërndarjes së dokumenteve biometrike të sigurta

Siguria e dokumenteve biometrike paraqet një prioritet kryesor për IdentiTek doku u fokusuar tek:

- Rritja e standardeve të sigurisë së dokumenteve.
- Harmonizimi me standardet dhe praktikat ndërkombëtare të ICAO.
- Reduktimi i rrezikut të falsifikimit përmes teknologjive të avancuara të personalizimit.

2.2. Përditësimi i Infrastrukturës dhe Teknologjisë & Projekti i Identitetit Dixhital

a. Teknologjia e prodhimit

- Rinovimi dhe zëvendësimi i pajisjeve prodhuese sipas rekomandimeve të auditimeve të kryera në IdentiTek SHA.

b. Siguria e Teknologjisë së Informacionit

- Zbatimi i rekomandimeve të auditimit Autoriteti Kombëtar për Sigurinë Kibernetike (AKCESK), (dt. 31.07.2023) dhe auditimeve të brendshme 2024–2025.
- Investime në firewall, SIEM, monitorim aktiv, enkriptim, backup, anti-intrusion.

c. Monitorimi i teknologjive të reja dhe përputhshmëria me BE

- Përshtatja me kërkesat e rregullores së Bashkimit Evropian (BE) eIDAS 1 dhe eIDAS 2.
- Përgatitja për implementimin e Portofolit Digjital (Digital Wallet).
- Harmonizimi me Rregulloren dhe Direktivat e BE-së për “Digital Wallet”, Rregullorja nr 910 23.07.2014 Parlamentit dhe Këshillit Evropian dhe direktiva 1999/93/EC e Parlamentit dhe Këshillit Evropian të 13 dhjetorit 1999.

d. Rritja e kapaciteteve operacionale

- Rritja e kapacitetit të prodhimit dhe efikasitetit të proceseve.
- Zhvillimi i produkteve të reja (p.sh. Leje Qëndrimi me Procedurë të Përsheptuar).

2.3. Rritja e cilësisë së shërbimit ndaj qytetarëve

Objektivat për vitin 2026 përfshijnë:

- trajnime të vazhdueshme për front-office;
- reduktimin e kohëve të pritjes;
- përdorim të teknologjive për matjen e kënaqësisë së qytetarëve;
- komunikim profesional, koherent dhe proaktiv.

3. Prioritetet Strategjike 2026–2027

3.1. Forcimi i sigurisë së informacionit

- Zbatimi i arkitekturës Zero Trust Infrastructure.
- Mbrojtje kundër sulmeve të brendshme dhe të jashtme.
- Përmirësim i vazhdueshëm i mekanizmave të monitorimit dhe reagimit.

Garantimi i mbrojtjes së sigurisë së informacionit ndaj sulmeve të brendshme dhe të jashtme (Maintain IT Security Protection Against Internal/External Attacks) është një proces i përdorur për të siguruar që informacioni dhe sistemet e Shoqërisë të mbrohen nga kërcënime të brendshme dhe të jashtme. Ky proces përfshin zbatimin e masave të sigurisë për të parandaluar, zbuluar dhe trajtuar rreziqet e sigurisë që mund të vijnë nga brenda organizatës (sulme të brendshme) dhe vecanërisht nga jashtë saj (sulme të jashtme). Rritja e nivelit të sigurisë së informacionit është një përgjegjësi e rëndësishme në një kohë kur kërcënimet e sigurisë janë të pranishme dhe ndryshojnë vazhdimisht.

3.2. Certifikimet ndërkombëtare

a. ISO 27001:2022

- Mbajtja dhe përditësimi i sistemit të menaxhimit të sigurisë së informacionit.
- Zbatim i politikave, procedurave dhe kontrolleve të avancuara.

Certifikimi ISO 27001: 2022 është një standard ndërkombëtar për sistemet e menaxhimit të sigurisë së informacionit. Ky standard ofron një qasje sistematike për menaxhimin e informacionit të ndjeshëm të një organizate, duke siguruar konfidencialitetin, integritetin dhe dispozicionin e tij. Për të mbajtur certifikimin ISO 27001 do të thotë që një Shoqëri duhet të plotësojë vazhdimisht kërkesat e këtij standardi, duke përfshirë implementimin dhe mbajtjen e politikave, procedurave dhe kontrolleve të forta të sigurisë së informacionit. Ky certifikim demonstroi një përkushtim për të mbrojtur informacionin e ndjeshëm, siç janë të dhënat personale dhe të dhënat e biznesit të konfidencialshme, nga kërcënime dhe vulnerabilitete të ndryshme. Për të njëjtat arsye është e domosdoshme vijimi i mbajtjes së këtij standardi për periudhën në vazhdim.

b. ICAO & ISO/IEC 7810

- Përputhshmëri me standardet ndërkombëtare për dokumentet e udhëtimit.
- Siguri e shtuar, dizajn anti-falsifikim dhe integritet i proceseve të personalizimit.

Organizata Ndërkombëtare e Aviacionit Civil (ICAO) cakton standarde globale për dokumentet e udhëtimit, përfshirë pasaportat. Për të përmbushur praktikën më të mira të ICAO është jetësore për qeveritë dhe shoqëritë që janë përfshirë në lëshimin e pasaportave. Këto praktika mbulojnë aspekte të ndryshme të dizajnit të pasaportës, tipareve të sigurisë, proceseve të lëshimit dhe mbrojtjes së të dhënave. Përmbytja e standardeve të ICAO siguron që pasaportat dhe dokumentet e tjera të identitetit janë të sigurta, të vështira për t'u falsifikuar dhe të njohura në mbarë botën. Kjo ndihmon në përmirësimin e sigurisë dhe parandalimin e krimit të pasaportave dhe vjedhjes së identitetit.

4. Projekti “Identiteti Dixhital për Shtetasit Shqiptarë”

Projekti “Identiteti Dixhital për Shtetasit Shqiptarë” përfaqëson një hap të rëndësishëm drejt modernizimit të sistemit të identifikimit elektronik në vend.

Projekti është një nismë kyçe brenda Strategjisë Ndërsektoriale “Axxhenda Dixhitale e Shqipërisë dhe Plani i Veprimt 2022-2026”, e miratuar nga Këshilli i Ministrave me Vendimin Nr. 370, datë 1.6.2022. Ky projekt synon të harmonizojë zhvillimet dixhitale të Shqipërisë me Rregulloren e Parlamentit Evropian nr. 910/2014 dhe të Këshillit Evropian të datës 23 Korrik 2014 mbi identifikimin elektronik dhe shërbimet e besuara për transaksionet elektronike (eIDAS), si dhe ndryshimet e saj nëpërmjet Rregullores së Parlamentit Evropian 2024/1183, e njohur ndryshe si eIDAS 2.0. Projekti synon:

- krijimin e identitetit dixhital të standardizuar për qytetarët shqiptarë;
- rritjen e sigurisë, aksesit dhe efikasitetit të shërbimeve publike dhe private;
- integrimin me tregun e përbashkët evropian dhe shërbimet ndërkufitare;

- modernizimin e infrastrukturës teknologjike dhe rritjen e transparencës.

Projekti është përfshirë në Listën Unike të Projekteve me Rëndësi Kombëtare, duke theksuar angazhimin e qeverisë për të modernizuar infrastrukturën dixhitale dhe për të përmbushur standardet ndërkombëtare për identifikimin elektronik. Implementimi i këtij projekti përshin zhvillimin e një platforme të avancuar për menaxhimin e identiteteve dixhitale, që do të ofrojë një mjedis të sigurt dhe të besueshëm për transaksionet elektronike. Kjo iniciativë do të ndihmojë në fuqizimin e qasjes së qytetarëve në shërbimet publike dhe private në mënyrë të shpejtë dhe të sigurt. Ky investim synon të krijojë një sistem identifikimi dixhital të standardizuar dhe të besueshëm, duke përmirësuar ndjeshëm cilësinë e shërbimeve elektronike në Shqipëri. Me anë të këtij projekti, Shqipëria synon të përmirësojë integrimin e saj në tregun e përbashkët evropian dhe të lehtësojë aksesin e qytetarëve dhe bizneseve në shërbime ndërkufitare. Projekti gjithashtu mbështet objektivat e dixhitalizimit të qeverisjes, duke promovuar transparencën dhe reduktimin e burokracisë.

5. Shërbimi i Kuponit Elektronik (e-Voucher) – Rritja e Përdorimit në vitin 2026

Kuponi elektronik (e-kuponi) është vlerësuar si një nga risitë më të rëndësishme teknologjike të IdentiTek, duke tërhequr vëmendjen e shtetasve dhe institucioneve shtetërore.

Ky shërbim, i lançuar në prill 2025, u mundëson qytetarëve të blejnë dhe të paguajnë online tarifat për kartën e identitetit dhe pasaportën, si në Shqipëri ashtu edhe përmes përfaqësive diplomatike.

Pas implementimit të suksesshëm gjatë vitit 2025, viti 2026 fokusohet në:

- zgjerimin e përdorimit të e-Voucher-it;
- rritjen e kapaciteteve teknike;
- integrimin me sisteme të tjera qeveritare;
- automatizimin e proceseve;
- reduktimin e kostove administrative dhe logjistike;
- përmirësimin e përvojës së përdoruesve.

Ky shërbim mbështet vizionin **“Shqipëria Cashless 2030”**, duke kontribuar në tranzicionin drejt proceseve tërësisht dixhitale dhe të gjurmueshme.

Vizioni shtetëror për të reduktuar ndjeshëm përdorimin e parasë cash brenda vitit 2030 ka sjellë një orientim të qartë drejt dixhitalizimit të proceseve financiare dhe administrative. Shërbimi i kuponit elektronik, tashmë i funksionalizuar, përbën një prej komponentëve kryesorë të kësaj transformimi. Ai mundëson kryerjen e transaksioneve të shpejta, të sigurta dhe plotësisht të gjurmueshme përmes kanaleve dixhitale si e-maili, aplikacionet mobile apo mesazhet SMS. Kjo jo vetëm që eliminon nevojën për kuponët fizikë, por krijon një përvojë të përmirësuar për përdoruesit dhe një model modern të administrimit.

Në fazën e dytë të zhvillimit gjatë vitit 2026, prioritet mbetet zgjerimi i përdorimit të e-Voucher-it, rritja e kapaciteteve teknike, integrimi i tij me sisteme të tjera institucionale dhe rritja e shkallës

së automatizimit. Përdoruesit përfitojnë duke kursyer kohë dhe duke shmangur procedurat fizike, ndërsa institucionet reduktojnë kostot administrative, logjistike dhe të prodhimit.

Ky përmirësim sjell gjithashtu avantazhe të qarta për mjedisin, duke reduktuar përdorimin e letrës dhe materialeve të tjera fizike, në përputhje me politikat e qëndrueshmërisë. Sistemi dixhital i e-Voucher ofron një nivel të lartë sigurie dhe gjurmueshmërie, duke minimizuar rreziqet e abuzimeve, falsifikimeve dhe humbjeve të kuponëve fizikë. Të dhënat e përdorimit monitorohen dhe analizohen automatikisht, duke mundësuar përmirësime të vazhdueshme, planifikim më të saktë dhe vendimmarrje strategjike.

Në tërësi, viti 2026 përfaqëson një periudhë konsolidimi dhe rritje për shërbimin e kuponit elektronik, duke e kthyer atë në një mjet të rëndësishëm në mbështetje të transformimit drejt një ekonomie moderne, të dixhitalizuar dhe në linjë me vizionin kombëtar për një Shqipëri “cashless”.

6. Vijueshmëria e Shërbimit: Disaster Recovery Site (DRS) & Zero Trust

6.1. Disaster Recovery Site (DRS)

Ambientet e Vijueshmërisë të shërbimit (Disaster Recovery Site - DRS) mundëson vazhdueshmërinë e shërbimit edhe pse në mënyrë më të reduktuar në raste situatash emergjente, katastrofash natyrore, apo edhe dëmeve të qëllimshme të natyrës fizike ose kibernetike (skenari "ransomëare") përkundrejt infrastrukturës ekzistuese.

Zbatimi i një DRS siguron funksionim minimal të shërbimeve kritike në raste emergjente, sulme kibernetike (p.sh. ransomware) apo katastrofa natyrore.

6.2 Zero-Trust Infrastructure

Arkitektura kompjuterike e bazuar mbi paradigmen "Zero Trust Infrastructure" parashikon implementimin e një niveli të lartë sigurie dhe autentifikim të thelluar për përqasjen kundrejt sistemit kompjuterik të shoqërisë. Kjo arktitekturë rekomandohet për mjedise kompjuterike që kanë të dhëna sensitive dhe impakt të madh në shërbimet publike që ofrohen qytetarëve pasi bëhet fjalë për sigurinë e të dhënave të qytetarëve.

Implementimi i Zero Trust parashikon:

- autentifikim të thelluar;
- kontroll rigoroz aksesesh;
- monitorim të vazhdueshëm;
- minimizim të riskut të penetrimit në rrjet.

Arkitektura është e rekomanduar për mjediset kritike me të dhëna të ndjeshme.

7. Projekti “Flag Ship”

Projekti "Flagship" është një iniciativë strategjike me fokus të dyfishtë: transformimin e përvojës së shërbimit ndaj qytetarëve dhe shërbimin si platformë kryesore për adoptimin e suksesshëm të Digital ID. Ky projekt ka për qëllim krijimin e një qendre zyre të avancuar që do të vendoset në një vendndodhje strategjike duke garantuar akses të lartë për publikun.

Zyra "Flagship" do të funksionojë si një model i shërbimit cilësor të Shoqërisë, duke ofruar më shumë se thjesht aplikime standarde. Funksionet e saj kryesore do të jenë:

Qendër Aplikimi dhe Kujdesi ndaj Klientit: Do të ofrojë të gjitha shërbimet standarde në një mjedis të rinovuar dhe modern, duke siguruar efikasitet dhe komoditet si për stafin, ashtu edhe për qytetarët.

Pika Qendrore e Digital ID: Ky është funksioni më kritik për vitin 2026. Duke qenë se shënon vitin e lancimit të Digital ID, "Flagship" do të shërbejë si një pikë informacioni, asistence dhe mbështetjeje direkte për publikun. Qytetarët do të mund të edukohen dhe të asistojnë në proceset e identifikimit dixhital, duke ndihmuar në reduktimin e barrierave teknologjike dhe duke nxitur besimin në sistemin e ri dixhital.

Shpenzimet kapitale të përlllogaritura nga IdentiTek, janë të dizenuara për të garantuar qëndrueshmëri dhe siguri operacionale.

8. PËRFUNDIME

IdentiTek synon të krijojë një ekosistem të qëndrueshëm, modern dhe të sigurt të identitetit kombëtar, të përputhshëm me standardet evropiane, duke rritur cilësinë e shërbimeve për qytetarët dhe sigurinë e të dhënave kritike.

Plani i Biznesit 2026 vendos themelet për një transformim teknologjik, operacional dhe organizativ të Identitekt. Investimet e planifikuara synojnë:

- garantimin e pandërprerë të shërbimeve publike;
- rritjen e sigurisë kombëtare përmes dokumenteve biometrike moderne;
- integrimin e Shqipërisë me standardet evropiane të identitetit elektronik;
- ngritjen e cilësisë së shërbimit ndaj qytetarëve;
- dixhitalizimin e proceseve dhe kontribuimin në objektivin kombëtar “Shqipëria Cashless 2030”.

Shoqëria mbetet e angazhuar në modernizim, inovacion dhe menaxhim të qëndrueshëm, duke garantuar shërbim cilësor, siguri të lartë dhe eficiencë financiare.