What’s Wrong with Diia?

The Government is overselling the Diia application trying to convince the Ukrainian citizens that it is the one and only means of the State e-services provision.
Question is that Diia has too many inherent issues in both architecture model and implementation quality.
Many Ukrainians feel something is wrong with it.
Ukrainian cybersecurity experts challenged Diia even before the first version saw light. Upon its public launch, they sound alarms about the app’s grave faults, insisting in and out of public view that current problems should not be tolerated.
Nevertheless, the Diia masterminds and designers keep giving blind eye to criticisms, which has already resulted in some risks being materialised.
Many Ukrainians already smell a rat but few people know what the Diia app issues really are.
To elaborate upon a “What’s wrong with Diia” theme we decided to cover them in a single document.
Feel free to share it by all available ways and channels if you second our reasons or have your own to be discontent with Diia app.

1. **Diia App Architecture Has Major Defects**
2. **Personal Data Processed and Stored in Diia App**
3. **Diia App Can Intercept and Collected Personal Data During E-documents Check**
4. **Diia App Can Be Used in Frauds**
5. **Diia App Can Spy Upon Users**
6. **Diia Installation Means Higher Risk of Remote Unauthorised Phone Intrusion (Hacking)**
7. **Diia Has No Opt-Out (Account Disabling) Option**
8. **Diia App Enables Rigged “Elections in Smartphone”**
9. **“Subpoena through Diia” Risk**
10. **Risk of Diia Operation without Internet Connection**
11. **Some Citizens Cannot Afford Using Diia App**
12. **System Too Centralised, Powers Too Aggregated**
13. **No App Use Rules, No Rule Compliance Monitoring Tools**
14. **Designers Ignored Laws and Regulations on Software Development**
15. **Diia App Unnatural Monopoly Established**
16. **No Public Access to Diia App Documentation**
17. **No Public Access to Diia App Source Code**
18. **No information on Diia App External Independent Audit**
19. **Diia App State Expert Appraisal May Have Been Biased**
20. **Diia Designers Do Not Communicate Properly With Users and IT Experts**
21. **Diia App Can Clone Documents Indefinitely**
22. **Diia App Utilisation by Various Organisations Lacks Transparency**

Experts who created this list if Diia app issues:

Andrii Baranovych
Andrii Pertsiukh
Artem Karpinsky
Kostyantyn Korsun
Kir Vaznytcky
Oleksandr Matsko
Roman Khimich

Major Architecture Design Errors

Diia app design violates a ground remote authentication rule: respective tools must be separated by trust levels.

Tellingly, Diia uses BankID, a software tool of just medium trust level to authenticate high trust level users such as digital passport bearers. It has been proven time and again that current BankID is vulnerable to low-tech attacks not providing enough security. In the financial domain, banks and financial organisations supporting BankID may indemnify their customers against losses attributable to BankID abuse incidents.

Still, the use of BankID for Diia user authentication defies a trust level separation principle. You can use high trust level tools to authenticate the users of e-services requiring medium or low trust level. You can also use medium trust level tools for authentication when a low trust level is sufficient. Diia app does it all the wrong way: low/medium trust level tools authenticate users of the most critical services, specifically, personal identity e-documents.

Such errors jeopardise the users of software and mobile applications violating the trust level separation rule. Any personal identity e-document, e.g. e-passport must be protected by the highest trust level tools only, which does not apply to current Diia app.

Diia App Stores and Processes Personal Data

Contrary to numerous public servants' claims, Diia app stores and processes personal data. Specifically, it registers, collects, adapts, modifies, updates, uses and shares personal data. It is clearly stated in the Diia site and in the Diia mobile app "Menu/Personal Data Processing Notice" section.

Quote

7. The Ministry for Digital Transformation (MDT) shall store the personal data as long as the personal data subject's account exists on Diia Portal but not longer than 5 years if any other storage period is not set by current legislation.

Unqoute

Diia Portal and Diia mobile applications are parts of the same system synchronising information so that the portal data are duplicated in the mobile app.

Additionally, experts demonstrated in public countless times that personal data are transferred between devices during the check.

Diia App Can Intercept and Collected Personal Data During E-documents Check

A phone can overtly copy passport data when reading e-documents. Refrain from showing Diia data to anyone except the uniformed police officer provided he presents his warrant card or numbered badge. The same data pass the MDT infrastructure but the processing procedure is unclear.

Diia App Can Be Used in Frauds

Currently, Diia app enables establishing a bank account remotely. It is on record that fraudsters logged in victims' Diia app accounts for illicit misuse to their own ends (unauthorised loans, purchases by instalments, other abusive acts).

Phone theft gives a free hand to the same misuse. Official statistics shows a monthly average of 4566 thefts (as of 2021).

Дія

Diia App Can Spy Upon Users

Diia state-owned company (SC) that belongs to MDT and supports Diia app and e-documents has an engineered capability to keep trace on the phones with Diia installed. Tracing may be provided either by Diia app or by servers that support the app and log all user actions, and app features use time and location. Neither tracing nor logging nor log processing are governed by any rules. Diia SC rejects any independent inspections showing lack of good intentions of the team designing and supporting the Diia app.

We mean by independent the inspections carried out by cybersecurity companies renowned globally, having sterling reputation and no ties with Diia designers or respective policy-makers. The inspection outcomes should be published stating clearly the scope ("what") and the procedure ("how").

Дія

Diia Installation Means Higher Risk of Remote Unauthorised Phone Intrusion

Government: When interested, the Diia provider can remotely install "an extended update" being actually a spy version on a Diia user's phone. The user will have no idea of being spied upon eventually in an illicit manner. The Diia app requires the maximum privilege level on the phone on installation (from camera and microphone to storage). It means that any update already has all the access rights without asking for authorisation. Third parties: Evidence shows that violators managed to get full-fledged control over the phone and all installed apps, and the owners were completely unaware.

Example. The Security Service of Ukraine (SSU) announced in 2021 that a group of violators was detained who made a speciality of mobile device remote hacking and illegal personal data collection. They charged $200 to hack a phone.

A mobile phone hacked by a third party is certainly a problem but Diia-installed phones give "bad guys" much greater opportunities when hacked.

Дія

Diia Has No Opt-Out (Account Disabling) Option

Any Ukrainian citizen having an ID card or passport equipped with a biometric chip (a document comprising a digital photo) can activate a Diia app account.

It does not matter whether the citizen wants to use the Diia account: the possibility is there anyway and an intruder can use it unknown to the legitimate user. At this point it is abused by fraudsters to steal loan funds steered to the individuals who for some reasons did not activate their Diia accounts.

This digital personality theft can be also used for many legally significant actions unknown to the individual, namely, residency registration, summons to court, real estate transactions, voting, etc.

The citizens have no digital documents-related risk management tools:

- disabling their account;
- disallowing activation of personal identity e-documents;
- refusal to use previously activated e-documents;
- alarm on an authorised attempt to activate a new instance of previously disabled e-documents.

Such features (Opt-Out option) would protect a citizen in disputes (related to illegal obtaining of a loan by social engineering, fraud, and end-user device (phone) theft or computer intrusion).

One effective countermeasure to Diia account abuse by third parties could be a requirement to perform the initial activation by applying in person at an Administrative Services Centre (ASC) bearing a paper/plastic ID. To add, a citizen should be able to legally "freeze" any Diia transactions, again by a personal visit to ASC.

It would be a good idea to have a tool to stop and log (with subsequent automatic notice to the police) any attempt of Diia use on behalf of a citizen who rejected this governmental service.

Ukrainian society has a strong demand for such risk-mitigating capabilities, and their implementation does not bring about any technical or organisational challenges. However, for some reasons the Diia owners are leery of offering those to the citizens.

Дія

Diia App Enables Rigged "Election in Smartphone"

Both President Zelenskyy and Minister Fedorov mentioned time and again voting with smartphones as their important goal. We can assume that they meant voting with the Diia app.

The deplorable experience with rigged "traditional" voting shows major risks there. This means jeopardy to national security and even coup attempt by doctoring on-line elections.

On-line elections are not capable of providing concurrently for secrecy of ballot, voting under no coercion and transparency of vote counting.

No country (except Estonia) has ventured to conduct elections on-line.

In April 2020, over 80 executives and leading officers of USA research organisations, academy staffers, and globally renowned experts such as Bruce Schneier and Martin Hellman published an open letter to Governors, Secretaries of State and electoral boards urging them "to refrain from allowing the use of any internet voting system"

45% of Estonian body of electors vote on-line; however, it took the country almost 20 years to develop their on-line voting model under the watchful eye of civil society, political parties and EU representatives. Along the way, many critical vulnerabilities have been detected in the on-line voting system, and the best experts improve it constantly. It works because the Estonian citizens have impossibly high trust in their Government, and its methodology basis is in stark contrast with that of Diia.

Дія

"Subpoena through Diia" Risk

Should the "automatic assured notice" on "advisements", "subpoenas", "summons to court", etc. be implemented and made legitimate, the citizens will run over the risk of falling victim to doubtful or illicit actions by the Government or third parties. However, this is also one of the proclaimed MDT goals. If achieved, it will aggravate the citizens' situation that is bad enough. Suppose that for some reason an individual stopped using the Diia app. Now it delivers a notice comprising summons to court going to hear this individual's property claim. The notice despatch is considered legally equivalent to actual notification. In case of default of appearance in hearing or untimely application for court seating rescheduling for any reason, the Government, fraudsters, "black registrars", etc. can engineer the court hearing against the individual.

Дія

Risk of Diia Operation without Internet Connection

Diia app designers keep saying that it does not store e-documents. The phone stores images containing document data but you have to be on-line to check if this is legitimate. Recently, the Kazakhstan Government reacted to mass protests by turning off the Internet. Apparently, this may happen in Ukraine too. If the Internet is down long enough the e-documents in Diia become just illegitimate pictures in smartphone. The same applies to some regions of Ukraine where the Internet connection is absent or unstable.

If you have to bear paper or plastic documents anyway, why bother installing and using an app?

Diia mobile app is a component of the Diia centralised system having a single point of failure. We have already witnessed many Diia service failures. Thus, such an important app can be brought down by turning the Internet off globally or locally (by jammers).

E-documents legitimacy must not depend in any way on Internet access or lack of access; the e-documents have to be self-sufficient.

Some Citizens Cannot Afford Using Diia App

You need a sophisticated phone to use Diia but not all Ukrainians can afford it. It is an issue, as some features are provided only by the app (e.g., vaccination certificates). Internet penetration in Ukraine is not 100%. Some people (especially elderly) find it difficult to enter PIN so their relatives either disable PIN or set codes like 1111. Diia with a simplistic PIN is unsafe. The designers cannot monitor every phone protection efficiency and rely on high individual cybersecurity awareness of the phone owners/users.

The proper use of personal identity e-documents requires skills not so common in Ukrainians, especially elderly. MDT offers neither formal User manual nor comprehensive guidance covering all critical aspects of e-passports and Diia app use.

The model where nothing but Diia provides Governmental e-services either prevents such citizens from using these e-services or exposes them to risks not offering any risk management tools.

System Too Centralised, Powers Too Aggregated

Diia administrators have enormous rights and no monitoring or controls. Some of them may be incentivised or coerced to collect information on certain aspects of citizens' lives and transfer it to third parties or allow third parties administrator-level access.

Excessive powers aggregation also prompts concern.

The recent incidents, such as Log4Shell and more widely known attacks, e.g. SQL injection may also be launched from the Diia Administrator level. This will harm or otherwise affect the citizens' personal data registries. It is possible for instance to create a query to any connected registry that changes, deletes or even destroys data being executed with Diia administrator privileges.

Intrusion into many Government sites compromised not only databases but also Diia portal software code and private keys to site domain SSL certificates. Those are the very certificates that protect your connection to the site. Even after these resources have been restored nobody took the trouble to re-issue SSL certificates. Such astounding ignorance brings risks of further sensitive user data (logins and passwords) leaks.

No App Use Rules, No Rule Compliance Monitoring Tools

MDT puts many Diia app use risks on users. The user's phone stores all his personal identity e-documents that are made legally equal to paper/plastic documents by the Law of Ukraine.

Notably, no regulation governs the app use rules, secure access requirements, use cyber-hygiene guidance, eventual compromise risks, etc.

Designers Ignored Laws and Regulations on Software Development

The legislation on Diia app operation is close to non-existent.

Formally, the e-documents are made legally equivalent to official documents by vague language in the Law of Ukraine No. 4335 "On amendments to the Law of Ukraine on the Unified State Demographic Register and documents confirming the citizenship of Ukraine, certifying the identity or a special status of an individual":

"E-passport is a Ukrainian citizen's passport in the format of electronic image of information contained in the Ukrainian citizen's passport".

However no Ukrainian law sets specifications and technological parameters of such e-documents, requirements on the application development and operation processes, acceptable technologies and their compatibility, facilities of the said processes monitoring (in particular, of public control), matching with current international standards and so on.

In addition, no laws and regulations set Diia security requirements: acceptable approaches and practices, control and testing stages, overall security criteria, independent safety assessment number and frequency, etc.

The Diia app is actually being developed and upgraded under MDT documents classified “For Official Use Only” and having no or limited public access.

It should be noted that software development commissioned by the Government is governed by the Resolution No. 869 “Approval of Common Requirements to Software Purchased or Created by the Government Order” dated 12 August 2009. With Diia, the said requirements have been mostly ignored.

This legislative indefiniteness has already resulted in prosecution of several individuals who developed apps having the looks of Diia but performed no intrusion to the Government IT infrastructure. Notwithstanding the ethical doubtfulness of their actions, they have violated no law. MDT actually provoked the emergence of such actions.

Дія

Diia App Unnatural Monopoly Established

The Ukrainian citizens are forced to use Diia having no other options.

For one, the vaccination certificates were available through Diia only for a long stretch of time although an alternative solution was ready months before the similar solution launched in Diia. The applications for UAH8000 sole trader lock-down compensation and “Covid 1000” also can be filed only through Diia.

Thus, an unnatural monopoly is being established with the only purpose of greater user acquisition.

Дія

No Public Access to Diia App Documentation

Diia app as an e-product lacks the following documents: user manual, general and technical overview, description of structure, features, operation model, applied technology, infrastructure, data transmission link structure, use rules, vendor warranties, compliance with personal data protection requirements, etc.

MDT either ignored expert’ and journalists’ requests for these documents or deliberately provided corrupted irrecoverable data. Tellingly, MDT stated that this information is classified “For Official Use Only”, although the app is public and distributed freely.

Дія

No Public Access to Diia App Source Code

Diia app designers have never published its source code.

An international best practice is to publish the source code, firstly, to show that there are no hidden functions for user surveillance, data collection on the phone model, operating system, day, time and location, use of certain app features, interaction with other software and apps, messenger use, browsing history, arbitrary retrieval of information from file system, etc.

Source code would be also a proof of (in-)capability to download upgrades for spying upon the users.

Дія

No information on Diia App External Independent Audit

Diia designers withhold information on independent external audit (appraisal) of the app.

According to international best practices, to avoid a conflict of interests a product should be tested by the experts not related in any way to its development.

To assure the users that the app is safe on a certain level of confidence, the auditors usually publish a report summary showing who (company and experts’ names), when, with what tools and under what methodologies carried out the security tests. Well-known international companies of good repute and high trust level in the expert community are usually considered most unbiased and qualified.

Not providing such reports means that either nobody tested (appraised) Diia app for safety or the testers were not so qualified and independent, or the expert conclusion was negative and contained many criticisms.

Diia App State Expert Appraisal May Have Been Biased

As any Government information resource, Diia must undergo the state expert appraisal and obtain a positive conclusion on an integrated information protection system design (IIPS) design and implementation.

Minister Fedorov misinformed the public on more than one occasion about IIPS Conclusion and deliberately provided illegible documents when asked for the Conclusion copy.

There is an evident conflict of interests (Head of State Special Communication Committee who signs the IIP Conclusion is nominated by the Cabinet of Ministers in the person of superintending Minister Fedorov) so the state expert appraisal would be expectedly biased. MDT keeps the IIPS certificate in the dark. It is still unavailable for the public although it is not and cannot be confidential.

Diia Designers Do Not Communicate Properly With Users and IT Experts

Diia app technical support is poor, hard to contact, and user complaints are mostly left unattended.

Notably, the average salary at Diia SC who develops the app is UAH 47,211. It is close to the average salary at IT businesses.

Brushing off experts' remarks on the app structure and operation drawbacks suggests that Diia project is rather about politics than technology.

The Diia project executives react to experts' criticisms in a rude, intolerant and boorish manner. Some public servants allow themselves to degrade and even threaten their opponents overtly. They would often say, "They put a contract on us" instead of sound arguments.

Diia App Can Clone Documents Indefinitely

The Government usually prohibits copying of paper/plastic personal identity documents, first of all, passports.

Document forgery is a major criminal offence. (Article 358 of Criminal Code: Forgery of documents, seals, stamps, and stationary; sales or use of forged documents, seals, stamps).

It is another way around with e-passports: the Government allows co-existence of equivalent copies on many devices, i.e. document copying/cloning.

The expert would ask in this connection; what is the reason why the approach is antipodal in this case?

How many copies of e-passport may co-exist: five, ten, one hundred or one thousand?

What MDT regulation specifies the number of copies?

Why has the personal attendance principle been rejected for e-documents? It is used in Estonia whose experience is praised by MDT. Traditional paper documents are handed over only in the very presence of the identified individual. It imposes liability on the officer releasing the document.

Will the designer officers bear any personal responsibility if somebody misappropriated an e-passport?

Diia App Utilisation by Various Organisations Lacks Transparency

After a single abuse case MDT banned e-passport use to MCO (micro-credit organisations). Tellingly, no regulation specifies under which conditions this ban would be raised or what criteria would be applied to use the ban on other organisations, e.g., postal service companies.

Дія

Kostiantyn Korsun

Cybersecurity expert.

Commanded the SSU cybersecurity unit and managed CERT-UA (at State Special Communication Committee); managed iSight Partners (an international cybersecurity company) Ukrainian office; as a third-party provider, rendered cybersecurity services to Symantec; co-founded a well-known Ukrainian cybersecurity company.

Delivered presentations on Ukrainian and international cybersecurity conferences and meet-ups: OWASP Ukraine, OWASP Kyiv, NoNameCon, BSides Kyiv, BSides Kharkiv, BSides Ukraine, UISGCON, Hack.Lu, RIPE NCC Days, IGF-UA.

Blogger and social advocate.

Andrii Baranovych

Ukrainian Cyber Alliance NGO Press Secretary.

Hacktivist. Blogger.

Andrii Pertsiukh

IT architect, volunteer, researcher, journalist.

Over 20 years of successful experience in banking systems development and deployment.

Artem Karpinsky

Ukrainian Cyber Alliance NGO President

Kir Vaznitcky

Telco and Fintech project consultant with 20 years of experience.

OSCE (Offensive Security Certified Expert).

Oleksandr Matsko

IT expert, volunteer.

Member of the Ministry of Defence of Ukraine Volunteer Council.

Roman Khimich

Researcher on digital environment security and trust, Telco market players' advisor, co-founder of Secure and Trustful Digital Environment Task Force Author of articles and presentations at PKI Forum Kyiv, BSides Kharkiv, etc.

Translated by Igor Dubinskyi