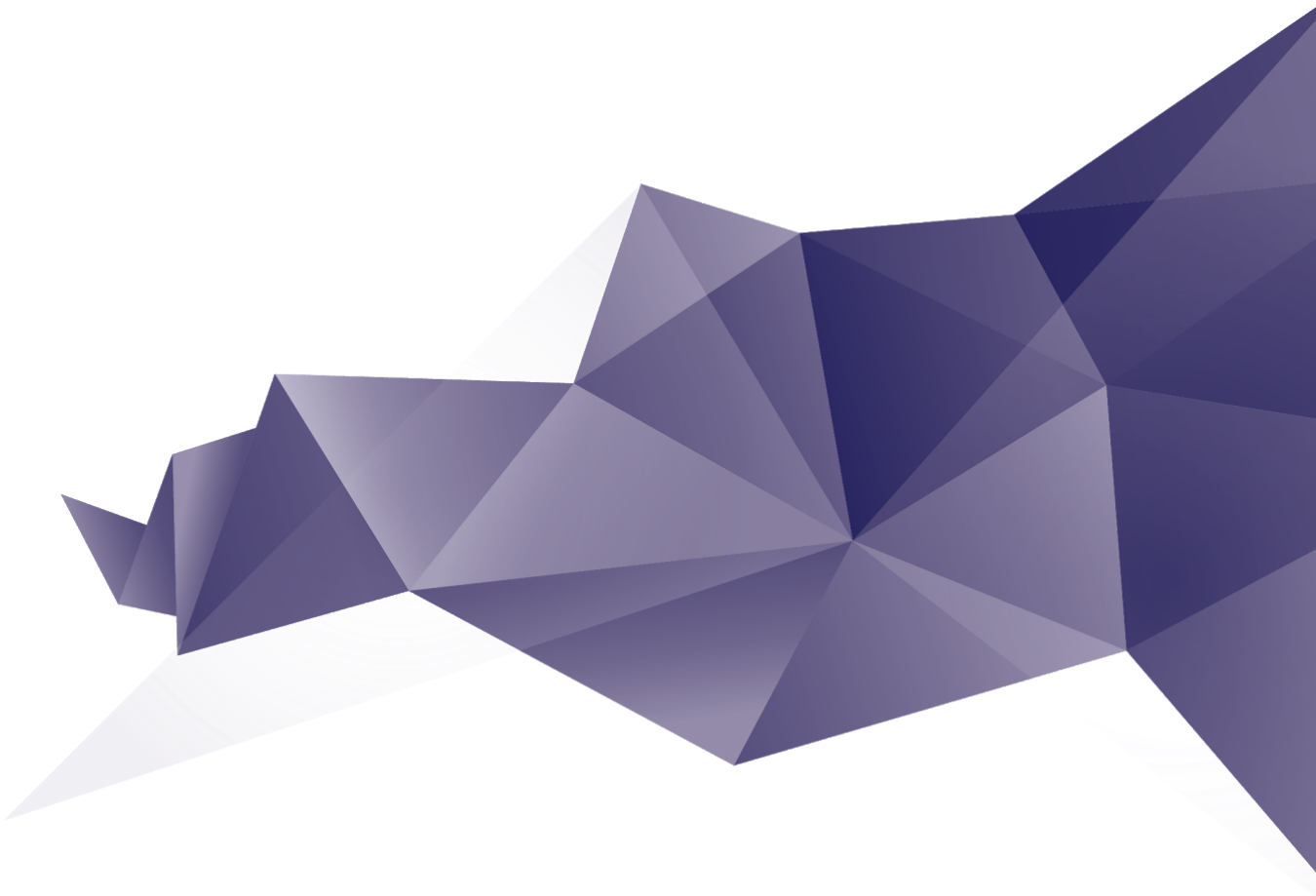


Privacy and GDPR Compliance of Least Authority's Private Periodic Payment Protocol (P4) Using Zcash

Client	Zcash (Zerocoin Electric Coin Company)
Authors	Greg McMullen, Silvan Jongerius
Reviewers	Liz Steiniger, Jean-Paul Calderone, Chris Wood, Meejah (Least Authority)
Date	October 26, 2018 Revised November 5, 2018 (1.2) Revised November 12, 2018 (1.3)
Version	1.3

Tech GDPR

Table of Contents

A. Introduction

Scope of review

Least Authority's Private Periodic Payment Protocol (P4) service enables anonymous payments for subscription services using Zcash shielded transactions. This paper reviews P4's privacy and data protection efforts through the lens of the European Union's General Data Protection Regulation (GDPR). It also reviews Least Authority's implementation of P4 and its efforts to fully anonymize the service to the degree that is technically possible, and when full anonymity is not possible, to minimize not just the collection of personal data, but to also minimize the *opportunity* to collect such data.

Subscription payments

Subscription-based business models have grown in popularity in recent years, and it is easy to understand why. Subscriptions offer a predictable, steady revenue stream, and enable ongoing work that would be too risky without ongoing support. A wide range of online and offline services now rely on subscriptions, as do charitable organizations seeking monthly donations. Major software bundles are now offered as subscriptions rather than as a one-time purchase, household subscriptions provide ready-to-cook food and other products, and patronage subscriptions support the creators of podcasts, webcomics, and other episodic content.

While subscription payments provide a practical business model, they come with a privacy cost. Subscriptions require that providers keep track of whether a particular subscriber has paid for their service, remind subscribers when payments are due, and stop service to subscribers who have not paid. Usually this will require collecting and storing at least some personal data about subscribers, including their contact information and payment details.

While the data collection and storage involved with subscription payments can be done in compliance with data protection laws, it still requires the collection of data. The growth of the subscription business model makes it even more difficult to participate in modern society without sacrificing the anonymity that was taken for granted in the era of cash.

B. Using P4 to pay for S4

Least Authority's S4 is a private, encrypted cloud storage service built on Tahoe-LAFS[1]. Least Authority plans to allow S4 users to pay using its new Private Periodic Payment Protocol: P4.

The goal of P4 is to provide a subscription payment option that is completely anonymous, collecting no data about the subscriber and leaving no possibility for them to be identified. This is not technically possible yet, but when perfect anonymity is not possible, P4 attempts to get as close as possible.

When a potential subscriber visits the Least Authority website and attempts to subscribe to S4, they will be given a choice between a standard credit card payment and anonymous payment through P4. If they choose P4, they will go through the following process to activate their subscription, make a payment, renew their subscription, or end their subscription.

This section shows how P4 works from two perspectives: the subscriber using P4, and the back end technical details.

1. Visit website through Tor

Subscriber view: The Least Authority S4 website is available through the public web or routed through Tor. If the subscriber is not already using Tor to access the Least Authority website, they are given instructions on how to download and use the Tor Browser.[2] Once Tor is installed, they are directed to a .onion web address that can only be visited through the Tor network. The subscriber is warned that accessing the .onion site immediately after browsing the standard website could make it possible to associate their initial visit with the Tor-routed visit, and is encouraged to come back later to finish the process.

Technical details: Tor[3] allows network location anonymous internet usage by encrypting traffic and routing it through at least three other computers running Tor before it reaches its destination. This layering of internet traffic is meant to make it extremely difficult to associate a specific user with specific activity online, as no one entity can see both who is requesting information and what information is being requested. Tor allows the use of protocol-specific URLs (.onion addresses) that can only be accessed through Tor.[4] Least Authority requires the use of Tor for accessing the S4 service and using the P4 payment system. While it may be possible to collect metadata about a user that could allow deanonymization, such as browser version or window size, Least Authority does not collect or store this information.

2. Get an invite code

Subscriber view: Once on the Tor-enabled site, the subscriber clicks a button to request a one-time use invite code.

Technical details: The invite code is generated by Least Authority using an application called *magic-wormhole*.[5] The invite code is displayed on the Least Authority website.

[1] https://tahoe-lafs.org/trac/tahoe-lafs
[2] https://www.torproject.org/projects/torbrowser.html.en
[3] https://www.torproject.org/about/overview.html.en
[4] https://en.wikipedia.org/wiki/.onion
[5] https://github.com/warner/magic-wormhole

3. Launch the client software and confirm the invite

Subscriber view: The subscriber launches *GridSync*[6], the client software required to access the P4 service. The subscriber enters their invite code in GridSync to connect to the service and complete the account creation process. The subscriber can use the service immediately after account creation, but a payment must be made within a set amount of time or access to the service will be terminated. The service can only be accessed through Tor, by way of a .onion address assigned by Least Authority.

Technical details: GridSync connects to Least Authority's servers through a Tor .onion address. When the subscriber enters the invite code, magic-wormhole sends encrypted configuration information to the GridSync client, where it is decrypted and used. Least Authority adds a subscription identifier to their internal database and associates that identifier with two pieces of information: a shielded Zcash address for payment, and a unique .onion address the subscriber will use to access the S4 service. If the subscriber does not make their payment, Least Authority can disable the .onion address to close the account.

4. Receive your invoice

Subscriber view: Least Authority creates an invoice for the subscription, including a shielded Zcash address for payment, the amount to be paid, the dates of the subscription, and the URL of the next valid invoice. The subscriber can view and verify their invoice through the GridSync client. Each invoice is cryptographically signed by Least Authority, and that signature is verified by the GridSync client. If the verification fails, the user is notified and advised on how to respond.

Technical details: The P4 "invoice" consists of a shielded Zcash address along with a number of defined fields that provide information about the requested payment. The required fields are: the currency name, the amount to be paid, the due date of the payment, the date the subscription will be extended to if payment is made, the name of the service the payment is for, the URL for the next invoice, the public key that will sign the next invoice, and the signature of the current invoice. There are also a number of optional fields that enable messages to the user, any credit that should be applied, and a version identifier. Least Authority uses the message field to communicate initial configuration information to new subscribers.

A complete invoice looks like this:

```
zs1z7rejlpsa98s2rrrfkwmaxu53e4ue0ulcrw0h4x5g8jl04tak0d3mm47vdtahatqrlkn
gh9sly?c=ZEC&a=0.1&d=1536064362&e=1538656362&l=Least%20Authority%20S4&u
=http://example.onion/86u4Cx1a&p=9eS4JZwugQmTcAFXDTQ5VKUzkKP01rKzfB_Sox
i4dhU=&v=1&s=GZWwXcxlh6kVUBoT67fudhpnJi1JJT7rZvQ0RCZXMA5LePUdXcq3lmeq_x
zOPdM2nua3kuPT9xPifiSKoc0=
```

The invoice is parsed by the GridSync client and the information is displayed to the subscriber in both a human-readable format and as a machine-readable QR-code to facilitate payments with cryptocurrency wallets that support QR-code scanning.

5. Make a payment

Subscriber view: The subscriber pays the invoiced amount by sending a Zcash transaction from their Zcash wallet to the address specified in the invoice. If the payment is successful, the subscriber's account is either activated or their subscription time is extended.

[6] https://github.com/gridsync/gridsync

Technical details: Subscribers can pay by shielded or transparent Zcash transactions, but Least Authority recommends payment by shielded transaction. Shielded Zcash transactions[7] use zero knowledge proofs to protect user privacy. Shielded transactions are completely opaque to everyone except the sender and receiver. Third parties can see a transaction has been made, but can't see the sender, the receiver, or the amount. The receiver can see the amount they received, but cannot see the sender's address. Least Authority maintains a Zcash full node in order to monitor addresses for payments.

6. Renew the subscription

Subscriber view: The subscriber is reminded of subscription payment deadlines by a notification delivered through the GridSync client, and can check other information about their subscription through the client as well. Least Authority provides a new payment address for each new invoice.

Technical details: The GridSync client tracks subscription dates and periodically checks for a new invoice at the URL provided in the previous invoice. A database of previous invoices is stored on the subscriber's device.

7. End the subscription

Subscriber view: If at some point the subscriber does not renew their subscription or fails to make an initial payment, their account is closed.

Technical details: To close an account, Least Authority will delete the .onion address that allowed the subscriber to connect to their account.

[7] https://z.cash/support/security/privacy-security-recommendations/#zaddr

C. Privacy and Data Protection Analysis

1. GDPR overview and scope

The General Data Protection Regulation (Regulation (EU) 2016/679) came into effect on May 25th, 2018 and seeks to regulate the processing and transfer of personal data of any natural person in the EU. Personal data under the GDPR is defined as:

> *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" (Art 4(1) GDPR).*

The definition of personal data includes users' IP addresses in some cases, as per the judgement of the CJEU in Case 582/14 – *Patrick Breyer* v Germany[8]. Following the same line of argument, most experts agree that a blockchain address would also constitute personal data, if it can be associated with an identifiable person. This includes associations made by combining data sets, so even data that appears to be anonymous can be personal data if it can be linked with other data to associate it with an individual.

Under the GDPR, "processing" is defined as:

> *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;" (Art 4(2) GDPR).*

In this evaluation, we examine if and where possible personal data is being processed in P4 and S4 to understand what may be in or out of scope of the GDPR. Where personal data is being processed, we evaluate the potential effects of the GDPR. Finally, we examine other possible impacts on users' privacy, even if the GDPR is not triggered.

There is a common misconception that encrypted personal data is not personal data and can be safely written to a public blockchain. The Article 29 Working Group has found encrypted data is pseudonymous, not anonymous. While it is unlikely that data encrypted using state-of-the-art encryption algorithms will be decrypted and linked back to an identifiable person using today's technology, future technology or undiscovered security vulnerabilities may pose a risk, and therefore that data must be treated as pseudonymous.

In the case of P4, data is also sharded[9], where the shards are distributed over different servers. In the light of the GDPR, this has to be understood as a technical measure in line with the requirements and state-of-the-art as explained in Article 32, but not as a means of anonymising the data and thereby moving it out of scope for the GDPR.

The Zcash addresses used to make P4 payments may be pseudonymised personal data, depending on the type of transaction made by the sender. There are four possible transaction types: public, shielding, deshielding and private[10]. In P4, the recipient address is always a shielded address, so

[8] http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945
[9] https://en.wikipedia.org/wiki/Shard_(database_architecture)
[10] https://z.cash/blog/anatomy-of-zcash

public and deshielding payments are not possible. The only two possible transaction types are shielding and private. Since the receiver does not see the sender's address in a private transaction, no personal data is visible and therefore no issue under the GDPR. A shielding transaction, however, would still identify the sender's t-address, and in some circumstances could be personal data. The sender's address could be personal data if the t-address has been identified in some other way, for example by the AML/KYC process on an exchange, and if the receiver has the ability to legally obtain that data.

2. Findings and concerns related to privacy and GDPR compliance

1. Logging IP addresses

IP addresses and other data may need to be logged to maintain the S4 and P4 services, and to ensure that any attacks are appropriately detected and mitigated. This logging may be slightly intrusive to privacy, but this intrusion is mitigated by the use of Tor.

As per Case 582/14 – *Patrick Breyer v Germany*,[11] IP addresses will under certain circumstances be considered personal data ("*a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person*").

If the Tor network is being used, the IP address that appears in the logs or servers cannot be related back to the user through normal legal or technical means. Therefore, Tor network connections should not be considered personal data, and are therefore out of scope of the GDPR.

2. File deletion, garbage collection

Despite the fact that all data stored on P4 will be encrypted and sharded by Tahoe-LAFS in such a way that it is difficult for anyone but the data owner to locate the data, it should not be considered anonymised. Unless the service is explicitly only made available for household use, it may contain personal data of third party data subjects and Least Authority will have to comply with the requirements of data processors as specified in Article 28 of the GDPR.

For example, if the data stored *could* be in scope of the GDPR, there need to be ways in place to truly delete data, and to control the retention periods of such data. Currently files are unlinked the moment they are deleted, much like how deletion happens on a regular storage device such as a hard drive. While this is by no means a perfect way to delete data, this is how the majority of the data controllers and processors under the GDPR will delete files, and it is expected to be sufficient. However, Least Authority should set up regular garbage collection policies and establish clear data retention periods, and communicate these policies to their users.

3. Consequences of maintaining a full node

Least Authority runs a non-mining Zcash full node to see when P4 payments are made. The GDPR consequences of running a full node are still uncertain, as both GDPR and blockchain are new and there have not been many decisions or opinions covering these issues. There is some chance Least

[11] http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945

Authority would be considered a controller or processor simply by operating a full node. CNIL, the French data protection authority, has issued an opinion holding that “miners” are data processors.[12] Least Authority is not mining with their full node, but if the opinion used “mining” as shorthand intended to cover the operation of any full node, there could be liability. Current guidance does not indicate liability for full node operators, but new regulations, decisions, and guidance from data protection authorities may change this in the future.

4. Wallet use and acquiring Zcash

Users must use Zcash to make payments within P4. However, like any cryptocurrency, the price of Zcash is highly volatile, so the price of a subscription is set in fiat. The price in Zcash is determined at the time of invoicing based on the exchange rate, and the Zcash amount is then paid with some (days) delay. It may be possible to identify users who make monthly transfers in the amount required to pay for a S4 subscription, identifying them as a likely S4 user. Cryptocurrency exchanges and projects raising money through ICOs[13] must take strict steps to identify customers to comply with anti-money laundering laws and other regulations, so it is likely the source of funds could be linked with an identifiable individual.

To remain fully anonymous, users could find alternative ways to acquire Zcash, or transfer larger amounts to a shielded address before subscribing. This could help hide their recurring payments, and also make their other uses of Zcash more private. Least Authority has no control over how its users handle their Zcash, but could take steps to set the price to commonly transferred amounts to allow users to hide amongst other transactions. Future versions of Zcash may allow receivers to require that payments come from shielded addresses, may make all addresses shielded across the whole network, or may include a technical possibility to require shielded transactions by the merchant. This is not technically feasible at the present because of the computational demands of zero knowledge proofs, but improvements in hardware and software should make zero knowledge proofs more practical over time.

Finally, Zcash shielded transactions can only be made with certain full-featured Zcash wallets.[14] The limited choice may lead to a correlation between wallet users or downloaders, and users of the P4 service. This is a minor risk to users but one they should be aware of when preparing to use any P4 service.

5. Integration of display of payment status in GridSync

The GridSync client receives the invoice and payment information and provides the user with information on when the next invoice is due and to what address it is payable. While this helps subscribers make sense of the dense string in the invoice, it could also be a potential vector of attack as there is another display layer involved. While not directly relevant under GDPR, the risk profile of the GridSync client will change with this integration. Any implementation of P4 will have to pay close attention to the signatures on invoices and to the integrity of the code interpreting the invoice.

6. Zcash Sprout versus Sapling

The upgrade from Zcash Sprout to Sapling[15] does not seem to have a major impact on user privacy in the context of P4. However, the significantly faster computation of zero-knowledge proofs needed for shielded transactions may encourage more use and thereby an more private network. In addition, it

[12] https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf (French)
[13] https://en.wikipedia.org/wiki/Initial_coin_offering
[14] https://www.zcashcommunity.com/wallets/
[15] https://z.cash/blog/whats-new-in-sapling/

improves the privacy features by allowing the spending key to be on a separate hardware device from the device that actually signs the transaction.

7. Time-based correlation when users switch to Tor from clearnet

When users visit the Least Authority .onion website directly after having visited the standard website, Least Authority (or a network or hosting provider) could collect data on the timing of the subscriber's visits to the clear text website and Tor traffic to the same site. This information could make it possible to link the user's real IP address to their Tor network traffic, effectively de-anonymizing them. This problem is worse when the service is not heavily used, and users can not hide in the masses. This is a privacy issue and not *per se* a GDPR issue, but any deliberate attempts at de-anonymisation could be an offence under the GDPR.

8. Tor .onion address as identifier

Every user of P4 receives a unique .onion address to access their files. Accessing a unique address could allow specific users to be identified, and could enable behavioural analysis of transferred ciphertext.

Least Authority has suggested that future versions could use a single .onion address for all users. While this would require a new solution for closing accounts when a subscription lapses, it would prevent the identification of individual users by their .onion address.

9. Analysis of metadata

There are two opportunities for metadata collection and analysis: during the web-based signup, and during use of the S4 service.

Certain information is exposed during signup, even over Tor. Operating system, browser version, screen resolution, and other information leave a "browser fingerprint", and can be de-anonymized with enough data points.[16] Least Authority does not collect this kind of metadata, but an application of P4 that did collect enough data to de-anonymize users would trigger GDPR concerns.

Metadata can also be collected during use of S4. While the data is securely stored and transferred as ciphertext between the server and the GridSync client, there is still a possibility that metadata, such as transfer size, frequency and patterns, are collected and analysed and could lead to singling out individuals or correlating with other clearnet actions. Due to the complexity and relative difficulty of relating this back to an already unknown user and actually identifying personal data, this is unlikely to be a GDPR concern.

10. Contacting support

When experiencing issues, S4 users are directed to a third party service (Zendesk[17]) for technical support. Zendesk requires that users leave their email address to get support. It is likely that Zendesk will collect other information about their users, including their IP address, geolocation, operating system and browser details, and information about their support issue. We recommend that Least Authority warn users that this information may be collected by Zendesk if they ask for support. To maintain anonymity, users could possibly use Zendesk through Tor, using a disposable email address generated for the purpose. However, preliminary tests have resulted in difficulties with this approach, e.g. refused network connections. Least Authority could also explore alternative, more private

[16] https://panopticlick.eff.org/static/browser-uniqueness.pdf
[17] https://www.zendesk.com/

communication channels for support purposes, such as encrypted chat services or use of Zcash's encrypted memo field.

11. Possible role of data processor

If users store personal data for non-household use on P4, Least Authority could be considered a data processor under the GDPR. Least Authority cannot access the data itself due to encryption and sharding, but this is considered a technical measure to protect the data. It does not move it out of scope of the GDPR.

Other providers of cloud-based storage take different approaches towards the GDPR. Some offer a data processing agreement/addendum.[18] Others claim that encrypted data is out of scope of the GDPR,[19] which contradicts the Working Party 29's opinion 05/2014 on Anonymisation Techniques. Some exclude the use of the service *"to collect, store or transmit personal data of any person without such person's consent"* through terms and conditions, most likely aiming to only include *household use* as a permissible way to use the service. [20]

Least Authority could exclude data processing activities that are in-scope of the GDPR through its terms and conditions, or make a data processing agreement available to its users to specifically include this use. However, some of the requirements of processors (Art 28, GDPR) will conflict with the private nature of the S4 service. For example, the GDPR requires that data processors keep a record of the name and contact details of each controller, and of the categories of personal data processed (Art 30(2)(a) and (b) GDPR). Least Authority may fall under the exception for organisations employing less than 250 employees (Art 30(5), GDPR), but it is unclear whether any of the following scenarios would annul the 250 employee exception:

- if the processing carried out is likely to result in a risk to the rights and freedoms of data subjects,
- if the processing is not occasional, or
- if "the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10".

Because client data is end-to-end encrypted, Least Authority has no visibility over what is stored on S4 and therefore it cannot be conclusively determined if the service is used for any of these purposes or not. The requirement of record keeping is upheld since the above three scenarios cannot be confirmed, and more importantly, they cannot be excluded.

12. Initial user base

Early in any implementation of P4, the userbase will be limited. This makes it easier to single out individuals or individual usage, as there is no hiding between other participants. Over time this should be mitigated by increased use of the service.

13. Usage of Tor

While Tor is widely believed to anonymise surfing, state actors have demonstrated an ability to compromise Tor connections by acting as nodes in the network.[21] Tor is the best approach for now,

[18] https://www.box.com/en-gb/gdpr
[19] https://tresorit.com/gdpr/cloud-storage
[20] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[21] https://advox.globalvoices.org/2014/07/24/russia-offers-4-million-rubles-to-crack-the-tor-network/

but it is only one piece of the puzzle, and Least Authority should continue to watch for vulnerabilities and ways to improve the service.

14. Recovery key

On top of the Tahoe-LAFS protocol, the GridSync client creates a recovery key upon signup that can be used at a later time to recover access to the data. While this improves the user experience, this also comes at the trade off of security. However, no particular GDPR implications are known to this solution.

15. Ease of use

Using P4 is not easy. Anonymity, not ease of use, was prioritized in its development. Right now, requires a working understanding of Tor, the process for acquiring cryptocurrency, Zcash shielded transactions, and so on. Improving user experience would go a long way to opening P4 to more use cases.

16. Implementations of P4 that do not use Gridsync

The Least Authority implementation of P4 is closely tied to the S4 service because of its reliance on the GridSync client. Gridsync is required to access the S4 subscriber's space in Tahoe-LAFS, and also receives and interprets the subscriber's P4 invoice. Other implementations of P4 will likely rely on something other than GridSync to handle P4 invoices. Fortunately, the invoice specification defined by P4 allows other implementations to avoid collecting data about the subscriber as long as the invoices are handled on the client side.

D. Conclusion

The Least Authority implementation of P4 does not likely raise any major issues regarding GDPR compliance, apart from the consideration whether or not to allow customers to use S4 for data processing under GDPR, and how to effectively prevent this (see finding #11). A few matters require highlighting as they may become an issue in the future as the usage of the service changes (finding #2), or the interpretation of the GDPR evolves further (findings #1, #3). The biggest concerns are related to the processing of data within S4, not within P4. The P4 protocol itself only presents concerns if subscribers insist on paying from unshielded addresses.

As long as Zcash transactions can not be linked back to a natural person, because they are private or because no link between the t-address and the user exists, the transaction within Zcash and payment information itself should be considered anonymous and therefor out of scope of the GDPR. However, such information could potentially become linkable in the future when more information about the address owner is revealed, making the t-address pseudonymous data, and therefore in scope of the GDPR.

Data in P4 is mostly anonymous, and only a few types of data could potentially be flagged as personal, and therefore in scope of the GDPR. The risk of identifying natural persons through the use of the service and could be mitigated by the use of zero knowledge proofs in Zcash shielded transactions. Other regulations, such as financial regulations, anti-money laundering regulations, and know-your-customer regulations, may be triggered by anonymous online services. New regulations around the world are attempting to make services providers responsible for their users' content.[22] It will be difficult to ensure the service is not used for illicit purposes, especially since Least Authority cannot see what its users are doing. However, these concerns are out of the scope of this analysis.

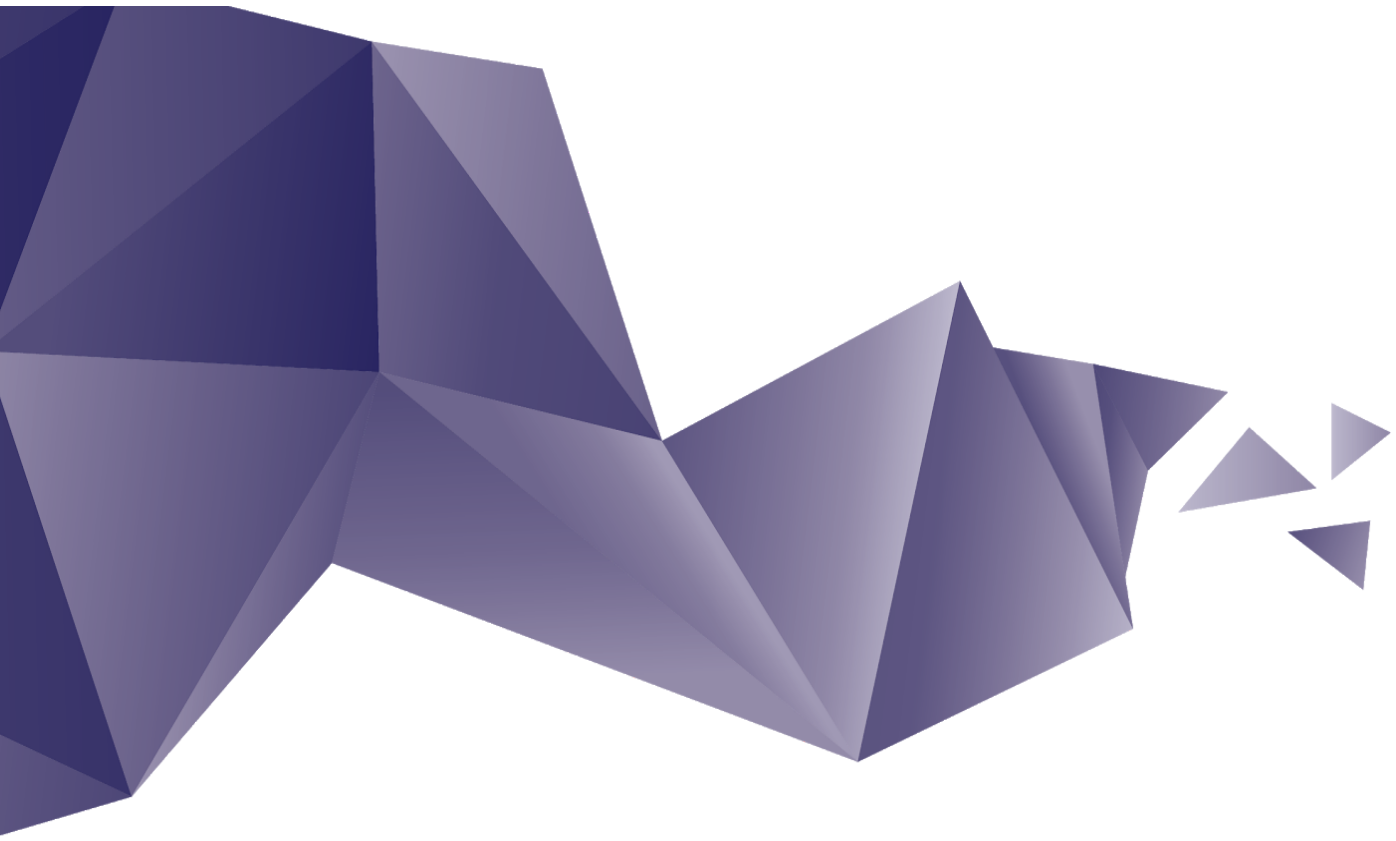
In our opinion, the P4 service allows for truly anonymous usage, or as close to it as you can get with current technology. However, the full benefits of P4 can only be realized if the user is extremely cautious with how they use it. Least Authority has tried to make it harder for users to make mistakes (i.e., by requiring Tor), however, it is still possible to gather some information through leaked metadata or trivial mistakes by the user that may, over time, be enough to link the usage back to a person. As the user base grows, it will become easier to be anonymous as it will be increasingly difficult to establish a relationship between specific users and their data or metadata.

Privacy-enhancing technology, including P4, is not perfect. It is difficult to use, and requires perfect handling by both the user and Least Authority. Still, technologies like P4 go a long way toward challenging the advertising-surveillance model of the modern internet, and illustrate how blockchain-based technologies could show a new way forward. Total anonymity may not be possible, but P4 demonstrates that we can get pretty close.

[22] https://techcrunch.com/2018/09/12/europe-to-push-for-one-hour-takedown-law-for-terrorist-content/

Disclaimer

TechGDPR is a technology and management consultancy company and has specific technical expertise in the area of blockchain technology. This document (the “Report”) provides information about Least Authority’s P4 and S4 services (the “Services”). The Report is based on the authors’ understanding of the Services at the time of writing. The Services are under active development, rely on experimental technology, and may have changed significantly since the time of writing. The Report is a technical assessment of the Services, but does not constitute or replace legal advice. The application and interpretation of data protection law and the GDPR is highly fact-specific. Seek legal advice about your specific situation before implementing any of the technologies discussed in the Report.



TechGDPR DPC GmbH

Rheinsberger Str. 76/77
10115 Berlin
Germany

+49 (0)30 5490 8661

contact@techgdpr.com
https://techgdpr.com

Commercial Register

Registered in the commercial register of the Charlottenburg District Court
[Handelsregister des Amtsgerichts Charlottenburg]
Registration number: HRB 195410 B
VAT No. DE317299781

CEO

Silvan Jongerius