

## Short Public Report

**1. Name and version of the IT-based service:**

Certified Privnote as provided via <https://certified.privnote.com> in September 2010.



**2. Provider of the IT-based service:**

Company Name:

Baladir S.A.

RUT: 2216406150019

<http://insophia.com>

Address:

Iturriaga 3429 Apt 1, 11300 Montevideo, Uruguay

Tel. +598 9 962 1374

Fax. +598 2 710 8711

Contact Person:

Jimmy Baikovicus | email: [privnote@insophia.com](mailto:privnote@insophia.com)

**3. Time frame of evaluation:**

October 25 2008 – September 2010

**4. EuroPriSe Experts who evaluated the IT-based service:**

Name of the Legal Expert:

Fernando Ramos Suárez LENER

Address of the Legal Expert:

Paseo de la Castellana, 23, 1º planta (28046) Madrid (SPAIN)

Name of the Technical Expert:

José Luis Rivas López HERMES SISTEMAS S.L.

Address of the Technical Expert:

C/ Santa Marta 52 1º (36202) Vigo (SPAIN)

**5. Certification Body:**

Name:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Address:

Holstenstraße 98, 24103 Kiel, Germany

**6. Specification of Target of Evaluation (ToE):**

The Target of Evaluation is the IT-based service Certified Privnote as provided at <https://certified.privnote.com>

The ToE does not include:

- Privnote web service provided in <https://privnote.com>
- External widgets and applications provided in <https://privnote.com>

## **7. General description of the IT-based service:**

Certified Privnote is a free web based service that provides users with a way to create encrypted notes. These notes can be shared over the Internet as one-time-use SSL URLs (hereafter also referred to as “links”) that expire after initial access via any web browser.

The service has been conceived as a fast, easy to use, fully end-user registration and password free service, in which users need only to learn the following actions to use it:

- create a note to get a link
- copy the link to the communication application of preference
- send the link to the addressee of choice

### Creating notes:

After filling in the note's creation form, the note's content is encrypted in the creator's browser with a random key and sent to Certified Privnote.

Certified Privnote then encrypts the received data with another random key, stores it, and returns this key to the note's creator.

Subsequently, the creator's browser generates a unique URL for accessing and decrypting the note by adding the two random keys.

The message is deleted upon the first retrieval of the generated URL. Consequently, if a user would like to use Certified Privnote to send the same note to multiple recipients, s/he will have to create several notes with the same content and then send each of the links obtained to the different intended recipients.

The note's creator is able to destroy the note by means of accessing it via the generated URL. This is possible as long as the note has not been read before.

### Sending notes:

Certified Privnote only allows the creation of a note and does not provide any form or method to send the note or – more precisely – the respective URL. Thus, the note's link exchange process has to be done by the note's creator "outside" of the Certified Privnote application (i.e., sending the URL by email, fax, SMS, phone, instant messaging, etc).

It is the full responsibility of the note's creator to ensure that the intended recipient receives the note's link, and that s/he is the one to finally read the note. Depending on the communication channel of choice, there may be a certain risk that third parties intercept the communication, get knowledge of the communicated URL and thus may be able to access a message in clear text.

### Reading notes:

Privnote guarantees that through the link any person can access the content of the previously written note. Once it is first accessed, the note's content is destroyed immediately and the link to the note becomes useless. If the URL is retrieved thereafter, the following sentence is displayed to the respective person: "The note you're looking for does not exist."

Since nobody can prevent the recipient of the note from taking a screen capture or even memorizing the note, Certified Privnote does not protect the note's content from being copied by the note's recipient.

A feature of Certified Privnote is the use of a technology that prevents the two keys that are used to create the link to a message from being shown in the retrieved URL. Rather, instead of the typical Certified Privnote URL containing both keys (e.g., <https://certified.privnote.com/n/nmbrtxdmqvburggw#efxxlcaulxxrohet>), the service always shows the following link in the address bar of the user's browser: <https://certified.privnote.com/n/destroyed/#destroyed>.

### Note expiration:

If a note's link is not used for a period of 30 days, all the note's data is automatically and fully deleted from Certified Privnote.

## **8. Transnational issues:**

The provider of Certified Privnote, Baladir S.A., is established in Uruguay whereas Certified Privnote's servers are located in the U.S. The service is offered via the Internet for any user and is available worldwide. This means that the users of the service may reside in any country around the globe.

## **9. Tools used by the provider of the IT-based service:**

- Hardware:
  - The servers are in Quad Core machines with RAID 10 storage
- Software:
  - Ubuntu Linux, Server Edition 10.04.1 LTS
  - Apache HTTP Server 2.2.14 + mod\_wsgi
  - Lighttpd 1.4.26
  - Django 1.2.3
  - PostgreSQL 8.4.3
  - Firewall: Shorewall 4.4.6 (iptables based firewall) in the servers and hardware based firewalls on the provider's routers

## **10. Version of EuroPriSe Criteria Catalogue for Experts used for the evaluation:**

Europrise Criteria Catalogue for Experts (Version 0.3)

## **11. Evaluation results:**

### ***11.1 Fundamental Aspects of Processing:***

The Certified Privnote service consists of storing a piece of information which can only be accessed with a "single-use" key (the link). Hereby, it enables its users to exchange encrypted messages in an easy manner. Processing user data, Baladir S.A. does not pursue any other purposes than offering the service.

The provision of the service results in the processing of the following personal data:

- Message data (encrypted content of the note)
- Cookies
- IP addresses

#### Message data:

The creator of the note can introduce personal data into the note. This data may even contain sensitive data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life (cf. Article 8(1) of Directive 95/46/EC).

However, as long as the service is provided as described above, its provider solely processes encrypted messages due to the fact that notes are already encrypted in the user's browser. The provider has no means to decrypt data and access them in clear text since it does not now the decryption key that is needed to read the message.

As Certified Privnote initiates the encryption of messages in the user's browsers, it may theoretically modify the overall service to the effect that it collects plain message data from its users. Consequently, message data do not only qualify as personal data in respect of users sending and receiving notes in clear text, but also in respect of Baladir S.A.

#### Cookies:

Certified Privnote uses session cookies to keep a session in the user's preferred language and to maintain the state of the "How does it work" help guide box.

#### IP Addresses:

Certified Privnote does not log IP addresses of users. Rather, IPs are solely processed to enable communication with Certified Privnote's servers. They are deleted as soon as they are no longer needed for communication.

Certified Privnote is the controller in respect of the processing of session cookies and IP addresses. By contrast, (professional) users of the Certified Privnote service qualify as controllers with regard to the processing of message data (cf. recital 47 of Directive 95/46/EC).

### ***11.2 Fundamental Technical Construction; Transparency***

Certified Privnote only collects and processes personal data that are strictly necessary for the purpose of providing the service. For both the creator and the recipient of a note it is possible to use the service without any registration. Message data is encrypted as early in the overall process as possible. It is deleted upon first-time retrieval of the respective URL or – if the URL is not retrieved at all – 30 days after the URL's generation. The service only makes use of session cookies. It dispenses with the use of persistent cookies.

Certified Privnote's services are described clearly to the users in the "About Page" that is available at <https://certified.privnote.com/about/>.

There is a Privacy Policy available on the Certified Privnote website. This policy provides information about the service in an appropriate manner. It informs users about personal data processed by Certified Privnote, makes them aware of the fact that the sending of the URL to the recipient may be – theoretically – intercepted by third persons and provides further privacy-relevant information. The policy also provides contact details to enable users' to contact Baladir S.A. in case of questions or complaints.

### ***11.3 Legitimacy of Data Processing***

Processing (encrypted) message data, Certified Privnote is bound by several provisions of Directive 2002/58/EC on privacy and electronic communications.

According to Article 5(1) of Directive 2002/58/EC, confidentiality of communications needs to be assured. Certified Privnote takes the following measures to prevent listening, tapping, storage or other kinds of interception or surveillance of message and related traffic data: Message data are encrypted

already in the user's browser. This means that their confidentiality is assured in respect of employees of Baladir S.A. as well as any third parties (i.e., even if someone could manage to gain access to the Certified Privnote database, s/he would be unable to read the notes since their contents are encrypted).

Confidentiality is also assured using SSL encryption for the exchange of information between Certified Privnote and the users of the service.

Details on the measures mentioned above are provided below in the section on technical and organisational measures.

In respect of users' IP addresses, Certified Privnote is bound by Article 6 of Directive 2002/58/EC. According to this provision, traffic data such as IP addresses of users must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. Certified Privnote is compliant with this provision due to the fact that it erases IP addresses on termination of a communication.

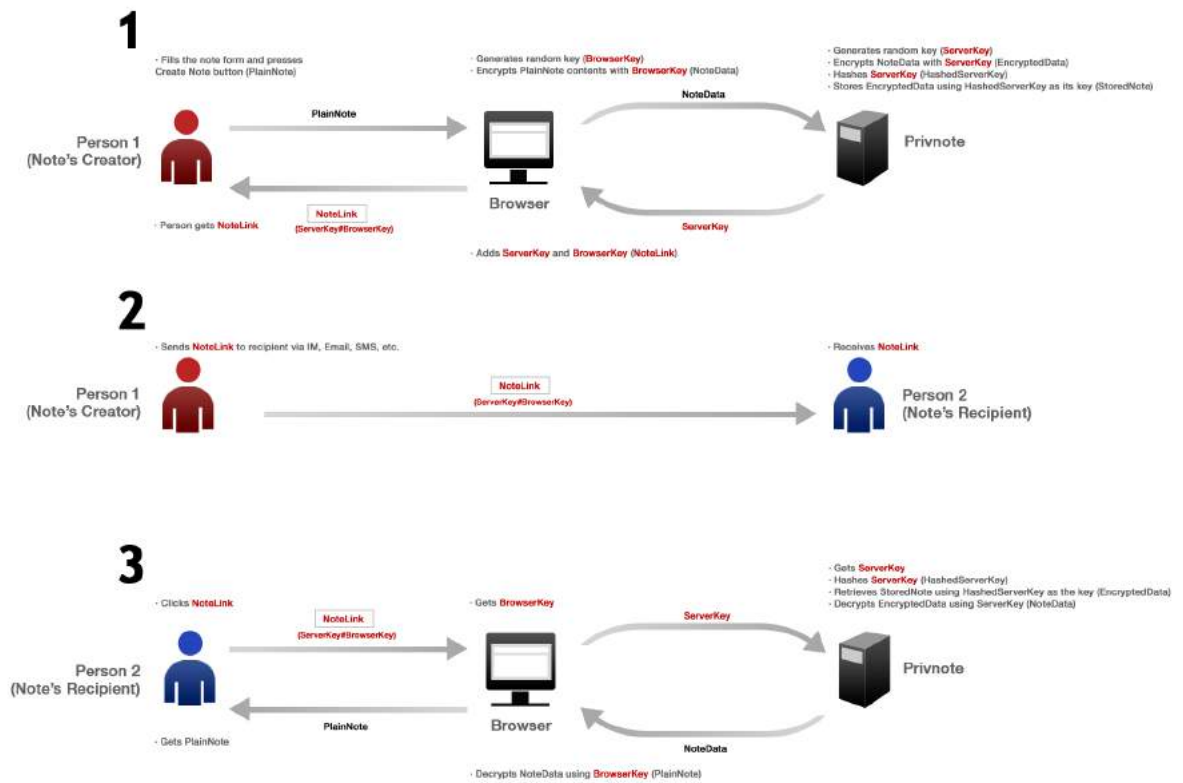
Certified Privnote servers are hosted by a professional hosting company that is located in the U.S. In respect of the hoster, encrypted message data do not qualify as personal data because the hoster does not have any realistic possibility to decrypt the data. However, as the hoster processes users' IP addresses on behalf of Baladir S.A., a processing security agreement has been concluded between Baladir and the hoster. The latter one provides appropriate guarantees in respect of technical and organisational measures of data security.

#### ***11.4 Technical and organizational measures***

All communication processes between the sender / recipient and Certified Privnote servers are secured using the SSL protocol to encrypt data that is transmitted over public networks. However, the exchange of the link between sender and recipient could be done using encrypted as well as totally unencrypted communication channels, because the sender alone decides about the means of transmission.



The following image shows the data flow and the encryption mechanisms securing the confidentiality of the message data. It is explained below.



Certified Privnote guarantees the confidentiality of the notes by using both, a browser and a server site encryption as well as an SSL transport security mechanism. The note encryption is a two-stage process:

After writing the note and clicking the “create note” button a java script – that runs in the user’s browser – generates a 16 character long random key which is used – together with the AES algorithm – to encrypt the note. Subsequently, the note is sent – via an SSL encrypted connection – to the Certified Privnote server. At this stage of the encryption process it is not possible for Certified Privnote to decrypt the message and to obtain knowledge of the note’s content.

On the server site – and as the second stage of the encryption – a 16 character long random server key is generated and used to encrypt the message again. This key is not only used for encryption but also as an index for the message.

After this key has been generated and the second stage of encryption has been finished, the server key is transmitted to the user – using the SSL encrypted connection – and combined with the browser key which was generated previously.

These two keys are combined to create the “link” which can be transmitted to the note’s recipient by means of e-mail, SMS, instant messaging, phone or other communication channels. As mentioned before the note’s creator is fully responsible for the secure transmission of the URL.

After receiving the link, the recipient can put it in the address bar of a normal, standard web browser and open the note. Therefore, the browser and the server key will be separated and the server key will be sent to Certified Privnote’s servers. Using the key the note can be found and decrypted – as a first stage of the decryption – and afterwards it is sent to the notes’ recipients. During this transport the note is still secured by the SSL encrypted connection as well as the first encryption that was done in the user’s browser.

After receiving the encrypted note the Java script uses the browser key – which is never sent to Certified Privnote – to decrypt the note. Thereafter, the note is presented to the recipient in plain text.

In order to provide a reliable and continuous service Certified Privnote production servers are backed-up with a daily and weekly snapshot of the entire system and the recovery procedure is tested regularly. The taken measures for back-up and recovery are appropriate and state of the art.

## **12. Privacy-enhancing functionalities:**

Certified Privnote encourages privacy by making use of data minimisation measures: No extra information besides notes’ contents and users’ IP addresses is required to use the service. Messages are deleted upon initial retrieval or after 30 days if they have not been retrieved at all. IP addresses are not stored but only used for the purpose of communication.

The service guarantees the confidentiality of the notes by using both, a browser and a server site encryption as well as an SSL transport security mechanism. Doing this, it positively stands out from conventional email services that do not provide any measures assuring confidentiality of communications at all.

**13. Issues demanding special user attention:**

Senders should be aware of the fact that they are fully responsible for the act of sending the link. They should keep in mind that – depending on the communication channel of their choice (e.g., email, fax, SMS, phone, instant messaging) – there may be a certain risk that third parties intercept the communication, get knowledge of the communicated URL and thus may be able to access a message in plain text.

**14. Compensation of weaknesses:**

Not applicable.


**15. Decision table on relevant requirements:**


<i><b>EuroPriSe Requirement</b></i>	<i><b>Decision</b></i>	<i><b>Remarks</b></i>
Data Avoidance and Minimisation	<i>excellent</i>	Certified Privnote cannot access the content of the notes, because the notes are encrypted and the users (creators and recipients of the notes) are the only ones who can decrypt the notes and access their contents. The service does not log any IP addresses. IPs are only processed to enable communication of users with Certified Privnote's servers.

Transparency	<i>adequate</i>	<p>Certified Privnote explains the use of the service in its About Page. It also offers a Privacy Policy that is available in English language.</p> <p>The service is described clearly and transparently to the user. No special knowledge is required to use it. All user information is up to date.</p>
Technical-Organisational Measures	<i>adequate</i>	<p>The technical and organisational measures that have been taken by Certified Privnote are adequate. Adequate physical access measures as well as efficient measures to ensure confidentiality have been implemented.</p>
Data Subjects' Rights	<i>adequate</i>	<p>The Privacy Policy informs Certified Privnote's users about all relevant privacy issues such as technical measures to assure confidentiality of communications, processing of IP addresses and usage of session cookies.</p>

## Experts' Statement

We affirm that the above-named IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Spain, sept 2010	FERNANDO RAMOS SUÁREZ	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Spain, sept 2010	JOSÉ LUIS RIVAS LÓPEZ	
Place, Date	Name of Technical Expert	Signature of Technical Expert

## Certification Result

The above-named IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT-based service facilitates the use of that service in a way compliant with European regulations on privacy and data security.

---

Place, date	Name of Certification Body
Signature	