Satswana Secure Email Service

This briefing is intended to assist those considering adopting the Satswana secure email service.

Hi, we want you to know how great this product is, and why it is the absolute answer to making your email secure from hackers and fraudsters. You will just want to know that it works and what is so special about it, so we will try and cover that – rather than talking techy, we hope that will help you use our product and keep your email safe. (You want the tech? OK, read the second paper!!).

We all love using email, but if we send sensitive personal or financial information without any protection there is an army of criminals trying to benefit by reading your stuff, you will know the problem.

The most important part of the answer to us is that it has to be easy to use, with the minimum of complication, and without requiring any specialist training. We expect you to find that this is so. Yes, you have to download an app, and if you choose to send the mail securely, then you have to press a different button from your ordinary mail, but that is it. The same for the receiver, it is as simple as that.

You use whatever email you are used to, with the email address you have always used, no changes there – of course you can also get it on your Apple, Blackberry or Android phone as well. Want to read the mail in a browser, you can do that too.

What we are doing is to make it impossible for your email to be read on its journey, and when it arrives we check that it is the same as when it left you, having made certain that the recipient is the person you intended to get it. We send you a receipt, so you know it got there safely.

The way we do it, we ourselves can never read your mail, nor do we ever hold the "key" that decodes it, nor do we store a copy, so we can never compromise your data or give it to anybody else – even a lawful authority has to get the content from either you or the receiver, we just do not have it, we only provide the security mechanism.

Please click here if you would like to register for a free trial, and thank you for your interest.

AND NOW, IF YOU WANT THE TECHY STUFF.

Regify, the technical bit

The purpose of this document is to give experts an insight into our products technical features.

Briefly, we encrypt (and compress together with all attachments) the data at the generating source and send the document to our portal where the (also encrypted) key is stripped off and forwarded to our independent Government owned registrar in Luxembourg. Note please that we cannot open the document, nor do we store it, the email only is sent on to the recipient.

This has several benefits over the gateway server option that holds the data, and encrypts it etc. First, we cannot be compromised as a consequence, secondly the data is absolutely encrypted end to end, thirdly we are unable to respond to any regulatory request for a copy, and finally if anything happened to our business, then you would still have absolute access to both your data and service.

We should stress that the registered email address is visibly authenticated, to optional levels, including multi factor SMS confirmation of identity so that only a properly registered address can receive the file based on a standard SSL connection. It cannot be opened without the request – which operates transparently to the user, all they have to do to read the mail is click a button (once they have registered and downloaded the app – or choose to read it in a browser). In practice this request sends a “fingerprint” of the document to the registrar, and provided it matches (proving that the document has not been tampered with) then the key is returned to automatically open the email, which also generates a receipt for the sender providing proof of delivery. Note please that neither sender, receiver, or indeed our service, ever know what this key is, so there is nothing for the customer to do, nor is an insider attack possible.

That is it in a nutshell, but we do have added bells and whistles, for example we can offer specific templates for invoices and payslips, and manage all services through a policy server if you wish. For those who use chat to negotiate we offer a non repudiable service, and similarly can offer collaborative document management with secure connections. If you wish you can white label the provision, just ask us please.

Now to provide you with even more detailed information, should you wish it.

The client setup installation includes the respective add-in for Microsoft Outlook and Mozilla Thunderbird. For IBM Lotus Notes, a special mail template is made available. RIM Blackberry users can retrieve their add-in with their web browser and simply install it. Apps for iPhone/iPad and Android are available in the respective app stores. The add-in provides the seamless integration in the work environment of the user and the organisation, respectively.

Satwana ensures the quality of the clearing services by working with globally respected providers that act as a trusted, independent Third Party.The clearing services are operated in fully redundant mode and in at least two geographically separate locations. All data processed is completely anonymous. For the clearing provider, this means that it neither knows the sender nor the recipient (e-mail addresses are not available), nor has the clearing provider got access to the contents. Thus, abusive risks are minimised.

Our products rely on established and proven standards, algorithms and cryptographic components for the processing of transactions. The following international standards are applied:

AES (Advanced Encryption Standard) is a symmetric algorithm used for encryption of the message (regify file) and for securing the transfer of information between the customer software and Satswana. Currently, the bit length is 256 bit. The bit length can be configured to accommodate future requirements.

RSA (Rivest, Shamir, Adleman) is an asymmetric algorithm used to ensure secure communication between the client software and Satswana. It is also used for identity files. Currently, the bit length is 2048 bit. The bit length and algorithm can be configured to accommodate potential future requirements.

SHA-2 (Secure Hash Algorithm 2) is used to hash the message and to anonymise the e-mail addresses of an addressee to the clearing service. All SHA-2 algorithms inside the process use 256 bit. The bit length and algorithm can be configured to satisfy potential future requirements.

SSL (Secure Sockets Layer) is used by the HTTPS protocol for secure internet connections. Satswana uses an SSL certificate applying the RSA algorithm with a bit length of 2048 bit. Bit length can be configured to satisfy potential future requirements.

FIPS PUB 140-2 and NIST SP 800-90 compliant random number generator is used to generate keys for message encryption and for the creation of session keys.Session keys are used for the communication between the user and Satswana as well as for the transmission of the key between the clearing service and the user.

The services core intellectual properties (IP) are protected by international patents that provide a solid legal foundation and its international applicability. These patents also ensure lowest total-cost-of-ownership in the market (for users and providers alike) and global scalability of the business.

The service complements solutions that are compliant with digital signature laws as it can be used to securely transmit any document, which of course, includes documents that carry a ”digital signature“. The regify service confirms the receipt of such a document and records it in an auditable manner, thereby providing additional evidence that complements solutions for digitally signed documents, it thereby increases the legal quality of any e-mail communication in any jurisdiction.

Given its end-to-end encryption, the services satisfy the legal requirements for data privacy and confidentiality. As a result, messages deliver on the major legal aspects of business communication being, first, guaranteed confirmation of receipt. By its very nature we provide indisputable proof of delivery (whether or not a message was opened). Ordinary solutions lack such clarity. Secondly, encrypted transmission where state-of-the-art encryption and end-to-end processes ensure that contents handled remain private between sender and addressee. Thirdly, the integrity of the contents is guaranteed since the system would recognise any manipulation and bring this to the attention of sender and addressee (by disabling the decryption of the manipulated content and notifying both parties). Finally, an auditable tracking log, since the web-based tracking log provides a user with the full audit trail of their transactions. The transaction history provides search functionality online.

It is important for all parties to recognise that the services are provided for use for lawful purposes only. They have been designed for global use in various jurisdictions. As individual laws and practices may require legal interception by authorised parties in order to be able to prosecute cases of abusive use, the solution enables Satswana to provide information under whatever laws, regulations and practices are applicable, thus ensuring that we are always legally compliant. An authorised party which has the right to legally intercept the communication must be in possession of the respective message. Assisted by Satswana, this party can then access the information of such a message and the clearing service will deliver the respective decryption key upon special request only. Please note that legal interception is an exceptional procedure between the clearing service and Satswana and will be recorded for reasons of auditability.

Many vendors narrowly define “secure e-mail” as encrypted e-mail, our comprehensive solution includes features such as confirmation of receipt and an auditable web-based tracking log of the transactions which elevates ordinary email to the level of a registered electronic letter. Our services make users more productive while ensuring security by automated processes.

Also, the separation of content transport and delivery and the management of security data automatically increases the level of security. Some solutions require hardware such as gateways, smart card readers and smart cards. Our simple email solution does not need any hardware, it was designed for any user of office software.

Copyright

The Satswana Team

Satswana Ltd
Tulip Trees, Church Road, St Johns, Woking, Surrey GU21 7QN
United Kingdom
Https://www.satswana.com