|  |  |
| --- | --- |
| Secure Phone: a new way of private voice and text communication A suite of new hardware and software technologies to protect your right to privacy of correspondence End-to-End EncryptionRSA 4096 asymmetrical keysAES-256 block encryptionA new key is generated for each sessionPrivate key (RSA) is generated on first activation and is securely stored on your phoneUsers can generate a new key at any time for any reason for additional security Custom kernelOur custom kernel includes only the absolute minimum required for functionality and has been designed with security as the primary consideration. MITM attack shieldWe implement our own algorithm for protection against MITM attacks. We do not rely on the conventional CA-authority. Our certificate is hard-coded into the software, CA-root private key is created on a computer with an air gap.Android basedAndroid-based proprietary features are kept to a minimum and are quarantined in their respective drivers.Peer to peer connectionVoice connection occurs in a peer-to-peer model directly between subscribers. In the case of symmetric NAT from yourISP, we use our servers as a proxy. All data is encrypted end-to-end.voiceless GSMGSM module is used only for the Internet connection. Flash SMS, MMS, SMS provider attacks and attacks with malicious programs sent via SMS/MMS are prevented by both the hardware and software.Random wifi MAC-addressTo prevent the collection of metadata on MAC-broadcast a random MAC address is generated on each unlock.No LoggingWe do not log any usage data on our servers or client devices. Servers are used only for communication and authorizing users. Only the attempts to attack our infrastructure are logged.Servers based on OpenBSD/FreeBSDAll servers run on the genuine Unix. Timely updates, well configured firewall, minimum set of software run by experienced security-minded professionals.FirewallEach phone has a statically configured firewall. The rules allow access only to our servers. All input and output ports are closed, all connection types except "new" and "established" are blocked. Our daemon does not allow anyone to change the firewall rules. App armour based on selinuxLimited set of applications. Only required software is installed (minimal Gentoo style).The access rights of these programs to the system and memory is rigidly controlled.Encrypted local dataThe key for stored data encryption is not contained in the hardware keystore. Each time the phone is switched on, the user must enter the key. While the device is active, the key is only in RAM store. Data encryption - AES-256. In ordinary phones, the key for encryption is generated when it is first turned on and stored in a special section of the read-only memory. If you change the password, only the master key is re-encrypted. In our case, when changing the password, the data is re-encrypted with the new keys.Panic PINPanic PIN to unlock the screen in case you are forced to enter the PIN-code. Erases alluser data from the device.HD voice codecsHigh quality voice codec.Minimalist interfaceThe interface is minimalistic yet complete, with a set of applications for the most used functions.Scratch card for activationScratch card to activate and recover a device.Scratch card is generated on the computer with an air gap. The scratch layer is applied using the PCI DSS standard. Scratch cards have no serial number. Subscriber's number is assigned after activation. Thus, no one except the person erasing the layer knows the number placed on the scratchcard and which number is assigned by the server.Switzerland based serversAll servers are located in Switzerland and protected by extremely strong privacy laws. A good team of Swiss lawyers awaits any challenges. Regardless, our servers do not and cannot store any correspondence or customer info.  | هاتف آمن : طريقة جديدة لتواصل آمن باستعمال الصوت والرسائل.مجموعة من تكنولوجيا المعدات والبرامج الحديثة لحماية خصوصيتك في التواصل.تشفير بين الطرفينالحروف غير المتطابقة لنظام التشفير RSA 4096تشفير باستعمال معايير تشفيريه متقدمة AES-256تكوين مفتاح جديد لكل جلسةيتم تكوين مفتاح خاص (RSA) لأول عملية تنشيط ويتم تخزينه بأمان في هاتفك.يمكن للمستخدمين إنشاء مفتاح جديد في أي وقت لأي سبب للأمان الإضافي.النواة المخصصةنواتنا المخصصة تحتوي على الحد الأدنى المطلق المطلوب للتشغيل وتم تصميمها لتكون آمنة في المقام الأولدرع هجمات MITMأنشأنا خوارزميتنا الخاصة للحماية ضد هجمات MITM (رجل في النص). لا نعتمد على السلطة التقليدية للشهادات. شهادتنا تم تصميمها بعناية في البرنامج. يتم تصميم مفتاح خاص في سلطة الشهادات الجذر (root) على جهاز الحاسوب بفاصل مادّي من باقي الشبكات.تصميم الأندرويدخصائص الملكية الخاصة بالأندرويد تبقى في حدودها الدنيا ومعزولة في سياقها.تواصل نظير – نظيرالتواصل الصوتي يحدث في نظام نظير – نظير (P2P) بشكل مباشر بين المشتركين. في حالة وجود ترجمة عنوان الشبكة (NAT) متوافق مع مقدم خدمة الانترنت الخاص بك نستعمل خوادمنا كوسيط. كافة البيانات تكون مشفرة بين الطرفين.نظام عالمي للتواصل بالهواتف (GSM) بدون صوتنظام GSM يستعمل فقط للاتصال بالإنترنت. يتم منع الرسائل الكاذبة ورسائل الوسائط المتعددة الكاذبة وهجمات مزودي خدمات الرسائل واستعمال البرامج الضارة في رسائل الوسائط المتعددة باستعمال البرامج والأجهزة.عنوان ماك (MAC) عشوائي لشبكات واي فايلمنع تجميع البيانات أثناء الاتصال بالشبكة يتم عمل عنوان ماك عشوائي في كل مرة.لا تسجيللا نقوم بتسجيل بيانات المستخدمين في خوادمنا أو على أجهزة العملاء. تستعمل الخوادم للتواصل وتأكيد هوية المستخدمين فقط. يتم تسجيل محاولات اختراق البنية التحتية فقط.الخوادم تعتمد على OpenBSD/FreeBSDكافة الخوادم تستعمل نظام يونكس أصلى. يتم تحديثه باستمرار في وجود جدار حماية منظم وكمية قليلة من البرامج يتم إدارتها بواسطة مجموعة من محترفي الأمان.جدار الحمايةكافة الهواتف بها جدار حماية ثابت. قواعد جدار الحماية تسمح بالدخول لخوادمنا فقط. كافة المداخل والمخارج مغلقة وكافة الاتصالات مغلقة ما عدا "جديد" و "مجهز". الإجراءات الخفية لا تسمح لأي شخص بتغيير إعدادات جدار الحماية.حماية التطبيقات في نظام سي لينكس (selinux).مجموعة محدودة من التطبيقات. يتم تنزيل البرامج المطلوبة فقط (نظام جينتو محدود). أحقية هذه البرامج في الدخول للنظام والذاكرة محدودة بشكل كبير.تشفير البيانات المحلية.مفتاح تشفير البيانات المخزنة ليس موجودًا في مخزن مفاتيح الجهاز. في كل مرة يتم فتح الهاتف يجب على المستخدم إدخال المفتاح. إذا كان الجهاز نشطا يكون المفتاح في مخزن الذاكرة العشوائية (RAM). تشفير البيانات - AES-256. في الهواتف العادية يتم تكوين مفتاح التسفير عند فتح الهاتف أول مرة ويتم تخزينه في مكان مميز من ذاكرة القراءة فقط، إذا قمت بتغيير الرمز السري يتم إعادة تشفير المفتاح الرئيسي فقط. في حالتنا عند تغيير الرمز السري يتم تشفير البيانات بالمفتاح الجديد.رمز بين (PIN) اضطراري.رمز بين اضطراري لفتح قفل الشاشة في حالة إجبارك على إدخال رمز بين. يتم مسح كافة بيانات المستخدم من على الجهاز.أكواد صوتية عالية الجودة.أكواد صوتية عالية الجودة.واجهة الأدنويةالواجهة تقدم الحد الأدنى ولكن بشكل متكامل في وجود مجموعة من التطبيقات للاستعمالات الأكثر شيوعا.خدش الكارت للتفعيلاخدش الكارت لتفعيل واستعادة الجهاز.يتم تكوين كارت الخدش على جهاز الكمبيوتر في وجود فاصل مادّي من باقي الشبكات. يتم تركيب طبقة الخدش باستعمال معايير سرية البيانات لربط البيانات الطرفية (PCI DSS). كروت الخدش ليس لها رقم تسلسلي. يتم إعطاء رقم المشترك بعد التفعيل. لذا لا يستطيع أحد معرفة الرقم الموجود على الكارت باستثناء الشخص الذي يقوم بالخدش وكذلك الرقم الذي يقوم الخادم بتوفيره.خوادم موجودة بسويسرا الخوادم تقع في سويسرا ومحمية بالقوانين القوية المتعلقة بالخصوصية. مجموعة جيدة من المحامين السويسريين ينتظرون أي تحدٍ. على كلً لا تقوم خوادمنا بتخزين أي معلومات عن العملاء. |

[العربيّة](https://www.emirates.com/dz/arabic/) – так вставляем в заголовке на сайте где языки