Pitch Deck for S-Company

"Cryptography Products that really work"

"Unbreakable, even if the life of Rothschild's youngest child depended on it"

"Private BTC address with Mircea's money encrypted and made public"

"Cryptography and air-gaped cybersecurity: safe AND usable"

"Open source and free for private physical person individual use"

Presentation by Mircea Digulescu
mircea.digulescu@mail.ru

22.10.2024

The Competition

- **VeraCrypt**: No cybersecurity features, standard primitives
- **Kaspersky** Endpoint Security: proprietary, probably good, but not great, standard primitives

- **NordLocker**: uses PKI for zero knowledge, no cybersecurity features apparently
- **McAfee Complete Data Protection**: proprietary, standard primitives

- **Trend Micro Endpoint Encryption**: proprietary, standard primitives, online, compliance
- **Symantec Endpoint Encryption**: proprietary, standard primitives, uses TPM, online, compliance
- **Sophos SafeGuard Encryption**: proprietary, standard primitives, **compliance**
- **ESET Endpoint Encryption**: proprietary, **online**

- **AxCrypt**: Filesystem only, No endpoint security
- **BitLocker**: Untrusted, uses TPM, registers keys to MS on Internet connection by default --> NSA
- **FileVault (Apple)**: proprietary, small block size, probably backdoored like BitLocker, Apple only.

- **PGP (Pretty Good Privacy)**: broken, untrusted.

Other "enterprise" products: IBM Guardium Data Encryption, WinMagic SecureDoc, Dell Data Protection Encryption (DDPE), Thales CipherTrust (formerly Vormetric), Boxcryptor, etc.

The Competition

On which would I bet by life / house?

The Competition

None.

The Problem

Trust

- Cryptographic Primitives
- Product
- Vendor
- Hardware / Firmware

Cyber Security

Basic Working Functionality

Advanced Features

The Problem

Trust::Cryptographic Primitives::Current Competition

* NIST "endorsed": NIST & DES, NIST & SHA1, etc.
* BlowFish replaced by TwoFish
* **"Here and for a while" mentality**

* **Forward security**: breakable in 5 years, means even what you encrypted today.
* **based on mathematical puzzles**
* maybe **vulnerable to new AI-enabled automatic SAT Solvers**: 7-rounds AES attack with 2^110 power.

:: https://tosc.iacr.org/index.php/ToSC/article/view/9713 [New Key-Recovery Attack on Reduced-Round AES]

* **photonic computing** (10^9 speedup): for the above results in 2^80 power, doable with a supercomputer.
* **PKI known vulnerable to quantum computing**: Shorr's Algorithm, etc.
* **Symmetric Key and Quantum Grover's Algorithm**: halving the key strength for find, 4x smaller for collision

The Problem

Trust::Product::Current Competition

* Open source code / Proprietary & obfuscated => trust vendor
  - Online => cyberhack probable, insecure almost surely
  - Proprietary and standards => for "compliance" mainly/only, trust vendor
  - Automatic Updates => trust vendor

The Problem

Trust::Product::Current Competition

* VeraCrypt is sole real viable open-source => still insufficient for air-gaped network security, but has flaws and no cyber: **rated Orange on NSA scale of difficulty (Vera+TOR), not Red nor Black**.

* Proprietary Vendors based in Western Block mostly, subject to **Wassenaar Arrangement Treaty** export licenses and vulnerable to court orders, gag orders => vulnerable or insecure products
* Corporate interest and kernel collusion: special interest groups => **self-censorship/buyouts** of encryption products
* **All use established popular cryptographic primitives**
  + None allow algorithm plug-in
    - Why if it doesn't matter anyway / can only reduce security? -> Export licenses: again, why granted if no extensibility allowed, but denied elsehow? => no extensibility, because vulnerable.
* **SafeHouse legacy software problem: master key generation based on system time.**

* **No end-to-end full product from a trusted Vendor**
  - Only VeraCrypt remains open source and trusted,
  - Partial Product => can be broken => inscure: with encryption, security is binary: is or isn't. No 99%.

* Many **vendors anti-trusted**: Microsoft BitLocker, Valut, Apple, etc.

* **Many for "compliance only"**

The Problem

Trust::Hardware/Firmware::Current Competition

* Hardware/Firmware Scenarios: trusted, partially trusted, partially untrusted, commodity (arbitrary)
  + No root => No trust
  + Root =/=> Trust.
  + Root, Faraday Cage, Air-gaped => maybe partial trust
  + Supply chain: TPM and commodity hardware no more than partially untrusted: would you bet your life on it otherwise?
  + Proven "special execution patter" hardware changes via a capacitor/transistor switch on repeated pattern

The Problem – The Full Need

* Cybersecurity Features
  - **Rootkit problem**

  - **Hardware/Firmware supply chain**: Must work in partially untrusted (preferably fully untrusted) settings.

  - **Minimal Functional Set:**
    * AIR-GAPPED NETWORKS: Including "getting data out of", "using data" and "updating/adding data".
    * Secure Online backups: laptops and PCs can be lost or stolen.
    * OS Isolation: Can't trust mainstream OSes, especially not Windows
    * Key Generation and Management
    * Data Wipping: SDD problem, OS problem, WiFi/Bluetooth problems

  - **Desired features:**
    * Importing online data
    * Working with encrypted data securely (Workstation mode)
    * Panic Kill-Switch that actually works
    * Vault timer perhaps? => Hard to implement
    * Functionality: Must not degrade security

The Problem – The Full Need

* Functionality (Basic)
  - **Do NOT contaminate trusted devices** when moving data to/from untrusted devices.
  - **Do NOT let vulnerable data touch untrusted devices, zones** (eg. plain secret keys, unencrypted data).
  - Detect compromised devices: **breach of trust**. Abort process on breach of trust (must be abortable).
  - Destroy vulnerable **burner devices / zones**: Wipping, Physical Pulverization, Melting
  - Change Encryption Key without Decrypting: Yeah, the actual encryption key, not via indirection. Why? Transit.

* Functionality (Advanced)
  - Web-ready:
  - A. Online Backup & Restore; Offline -- path to --> Online with selected data.
  - B. Secure Communications: Email/Telegram like
    * End-to-end not really solved: dependent on PKI and Trust with WhatsApp, spread key with Telegram.
    * Nickname signing.
  - C. Secure Content Delivery Network: Webhosting and Webdelivery (plain content). Change key.
  - D. Secure Key-Value Database with SQL Queries.
  - E. Block-chain Ready

The Competition

Which from the 10-15 products covers at least the basis of these?

The Competition

None.

* - This means in practice there is currently no off the self encryption product out there: they all have critical lackings, breaking security of encryption

The Solution

Can S-Company and SKREM Suite really cover all of these?

* “We succeed where others fail, we deliver where others deliver excuses”

The Solution

Cryptographic Primitives: New large-circuit primitives based on SKREM-like ciphers:

* Can be combined safely with AES, ChaCha, etc. --> suite will support this

* Circuit size on order of 2^64 nodes (versus ~2^24 for AES-256)

* Circuit different for each encryption, from a family of 2^4294967296 (versus 2^0 for AES)

* Security based on indirection operation and Chaos Theory

* Is a Kolmogorov Extractor generating new randomness

* Not a short-block cipher: with 1 Gbyte salt, block size is 2-100 Megabytes

* A lot of functionality features doable

* See "Hiding Data in Plain Sight" and "Applications of SKREM-like ciphers" on https://www.matsoft.ro/Matsoft__Research62__Computer_Science_113.html

(peer reviewed, with abstract and links)

+ Concrete SKREM variant is to be chosen based on experiment (running time tradeoff)

See https://www.matsoft.ro/Matsoft__Products62__SKREM_Suite_113.html for ampler product description

The Solution

Cybersecurity Features

* Can we do all the minimal requirements as highlighted before? + **Yes we can and yes we can**.

* Even with **Commodity Hardware**? **Yes**, under some partially untrusted or better scenario yes. Even with full non-trust, PROBABLY yes (relies on trust verification). With commodity hardware from 2010-2020. With 2021-2024 maybe, with 2030 who knows?.. but still , probably yes, when proper precautions possible and taken.

  + Are you sure? Yes. The technical details I have in my mind.. **I found solutions for all core steps.**

  + Will it be easy? For stage I, yes. For stage II, it will be somewhat easy but it will cost. For Stage III, it was hard to come up with working solutions for all.. but it is done; just implementation is required (based on SKREM) - this will be much harder, but possible for sure.

  + Are you really really sure? Yes, given the state of the 2010-2020 and maybe 2020-2025 commodity hardware, I am sure.

* What are the key ingredients of how?

  + **MicroSD cards**, **QR Codes**, **Trimmed down** distribution of **FreeBSD** (not Linux for licensing reasons)

  + **SOFTWARE FEATURES**!!!: zero knowledge data transit features, key management, long key decrypt, data integrity validation, etc. <-- all area required just for simple scenario of Node security storing unbreakable encrypted data.

* How do you beat backdoors and firmware/hardware backdoors? + I will tell you after you invest. But here's a hint: The key lies in the number of transistors.

See https://www.matsoft.ro/Matsoft__Products62__SKREM_Suite_113.html also.

MAT SOFT

The Solution

Functionality (Basic): this is basically required to achieve other business goals. **Yes, all of those can be fully achieved**.

Functionality (Advanced):

- A. Online Backup & Restore.
  * Yes, can do. All ideas clear, just implementation required.
- B. Secure Communications: Email/Telegram like
  * Yes, can do. Yes, I mean it.. fully. With symmetric key encryption. Not easily, nor as fast as Telegram, but yes, can do. Unbreakable (unless key exchange mediation server compromised live, if used).
  * Key Exchange: offline channel, satellites, quantum or mediated by exchange server.
    + Will be combined with Diffie-Hellman, but just as an obfuscation step.
    + Other idea: Adversary delay handicap amplification.
  * Source / Destination anonymity (yes, better than Telegram even!).
  * Dicoverability: initially on Well Known Locations (WKLs): blockchains?
  * Routing: now that is a bit harder. Currently all must get all. So possible, but slow and high bandwidth.
  * DNS: dependent on routing. So yes, possible.
  * Source obfuscation: Only at Ethernet ring level: so, currently, still WiP. But if broken, content of messages is still secure: so long as the receiving party is not compromised.

MAT SOFT

The Solution

Functionality (Advanced):

C. Secure Content Delivery Network: Webhosting and Webdelivery (plain content). Change key.

* Again, wow, yes, can do. How anonymous? You request content id XXX and say give it to me encrypted with key YYY. And then it happens. In transit it is impossible to tell which content you requested. Server does not know what content ID XXX contains. It changes its encryption key to YYY without seeing the plain text.

+ DMCA enabled: content ID xxx can then be removed by webhoster. Reupload with different key is of course impossible to defend against, as with any system.

+ "torrent tracker": maybe in the future -- based on content hash, not content ID.

+ Stored content "recycling": without ever needing to fully decrypt or have decrypted data on HDD.

D. Secure Key-Value Database with SQL Queries.

* In the future. Problem not yet fully considered. FHE maybe later.

The Solution

Functionality (Advanced):

E. Block-chain Ready

* **Yes, sir.** Domain of K-Company (see K-Company Pitch).

+ **Fully hidden transaction chain until amount spent needs to be proven**. Proof can happen biliaterally and be stored for later usage. Yes, fully hidden: not even the original sender knows when you have spent the funds, with full blockchain access (except when you reveal the transaction chain).

+ **Large mandatory "casino" mixers for miners** ==> ownership over an address can be dilluted fast. And yes, it works. It has EV almost 1, and SDev not too large. Yes, it works with symmetric key. Yes it works DeFi. Yes it works without even the participants knowing "who got which output" (except their own!).

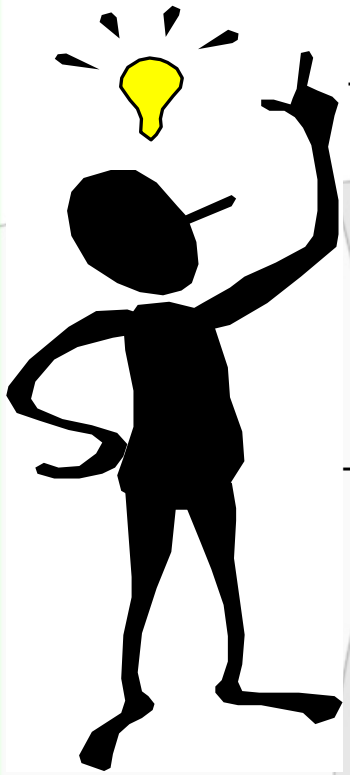
+ **Security based on SKREM**. No PKI Quantum Computer vulnerabilities. Conjectured provably unbreakable security for a Turing Machine (within key strength).

* Strive to resolve overconcentration of capital with BTC: vulnerability for any future BlockChain not only economic.

See https://www.matsoft.ro/Matsoft__Startups62.html for all S,K,R,E,M,F companies.

Uses Cases

<u>Idea in a nutshell</u>: Yes We Can. No other current or prosepective product can (or aims to) but S-Company can and will.



+ Securely storing valuable data (crypto private keys, familiy photos, etc.), even online. No graveyard.

+ Protecting sources as a journalist / transiting with sensitive data

+ Storing private data such as PII / PIII.

+ Storing membership lists of secretive organizations, like masonic lodges, syndicate memberships, etc.

+ Planning political activity: prevent ear damage

+ Storing military grade launch / abort codes and/or troop dispersal data (eg. as a result of EOB).

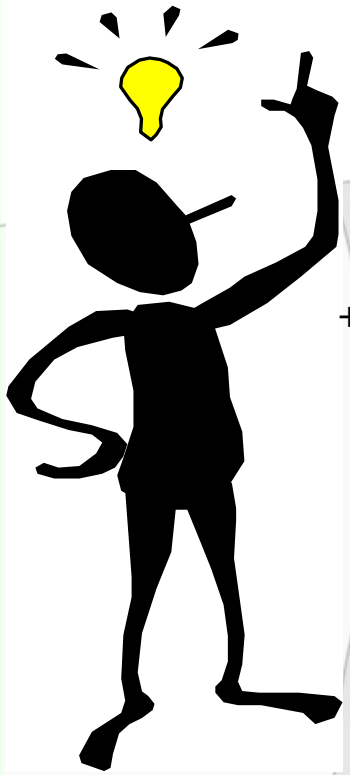
+ Chatting securely with known parties (after offline contact).

+ Chatting securely with strangers: so far as the stranger's device/keys are not compromised.

+ Spreading news Behind Enemy Lines (BEL): Imagine having RT.com and SputnikGlobe.com back in the EU.

MAT SOFT

Uses Cases



Block-chain related

+ Store value

+ Serve as a WKL (Well Known Location) for global sync / dns.

+ Store short data as backup

+ Make transfers / send messages almost fully anonimously.

Future

+ Coordinate between people (including strangers): locations, people, movements, and actions

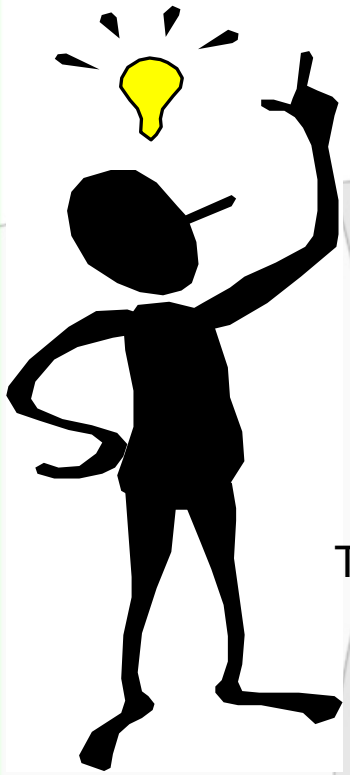
+ Finance and Coordinate own economic circuts without the need for banks

+ Implement Dead Man's Hand "heartbeat" systems

+ Others.

The Product

Can we really? Yes, we can.



Why didn't others do it already then?

- Because they don't want to
- Because they did not know about SKREM-like ciphers and other innovations
- Because they don't get investments

In fact, I am already working on it.

The scientific part and technical parts, except a few minor details for advanced online features, is fully clarified. To the point that I know how I want the code to look like etc.

MAT SOFT

S-Company: why raise capital?

1. I code slow.

   + After doing Phase I myself, I want to delegate as much as possible code writing - and still retain and do the crucial code reviews. If I don't get money, I will do it myself, but it will take years, up to a decade.

2. Monetization is further down the stream, not immediate.

   + I don't want to stay poor until I become crypto billionaire in 10 years. I am already 39.

3. I need money for promotion.

   + Advertising

   + Partnerships

   + Paid security audit by independent auditor of product suite

   + Paid evangelism / crypto popularization

S-Company: why raise capital?

4. I need money for OS customization stuff.

+ I will just code review. No need to learn FreeBSD from scrach myself.

5. For advanced stages (so for Web features, after Phase III), there is quite ample technical work. Maybe 3-4 man-years to get to a viable MVP. Especially with experimenting and all. For phase II, probably 2 man years. This costs. If I don't have money, I will have to do it myself while bootstrapping: so like at 0.2 man years / year. Very slow.

6. Purchase Advance Monetization. Software needs to remain open source code (not free, but open source) for Trust reasons. Affects monetization.

+ I would rather my prospective customers donated upfront: then they can support, see and modify source code when product is ready.

+ There will be no technical copyright protection measures on the product(which would be circumvented with/without help of CIA/NSA anyhow). It will also work in disconnected mode.

S-Company: why raise capital?

7. Politics.

+ I will face adversity from CIA/NSA and the like no doubt, for no legal reason. I need to have money to live properly and securely outside any potential harm.

+ Note that I was already Assanged for a good couple of months in 2023 in Germany: although I managed to get out of that situation alive and well, and continuing my activism, if it happened a second time I don't think it would be resolvable.

8. I want to focus on this full time.

S-Company

It will get done anyway: with or without investment.

Without it will be much slower, so yes, please donate/invest/advance buy.

Disclaimer: Neither investment/donation/advance buy is any 100% guarantee anything will get done. I might get killed, married, embedded in some non-Western structure, etc. However, getting money exponentially increases the probability at least SOMETHING will get done. Nothing in this presentation is nor should it be regarded as investment advice. Your capital is at risk. Only donate/invest/advance buy amounts you can risk and which you consider are lost forever when sent. Donate only for appreciation of myself, not as an investment nor advance buy. Advance buy presents risks the product might never occur. There are no refunds.

Note: The above is mainly to deal with hostile investors/donators/buyers - like groups and people actually seeking to have product NOT become a reality. But it is not only for that purpose, so please read, acknowledge abide by it.

S-Company Initial Team Plans

Team Plans with money:

- Currently Mircea Digulescu.
- Probably **2-3 software engineers** will be added.
- Work on OS customization (FreeBSD) will be initially outsourced.

- Another like **1-3 non-tech people**: **secretarial**, administrative, accounting, **legal**, etc. Helps with Politics of getting settled in a jurisdiction.

- Also I need at least like **1 marketing person for online**.

- So mid-level team will probably be like: **me + 3 internal engineers + 2 non-technical staff + 2 contractors for OS**

When advanced WebSuite stuff happens, then probably **1-2 more on front end side** and **2 more web software engineers**.

- After MVP completed, theoretically team could be cut fully. However, better to keep them, since they will not be too costly.
- Note: The main added value is by Mircea myself: core parts of Phase I, work breakdown, code review, guidance and specs, leadership, etc.
- So no need for advanced algorithmics stuff or innovation on behalf of engineers. We need **competent engineers who can code**. But what to code and getting it right is Mircea's part.

S-Company Initial Team Plans

Team Plans with money:

- Without myself on board, I would not trust a team of 4 codeforces even to get this done right.

Block chain: Except basic primitives it is the perview of K-Company (see the related pitch).
So no expenses will be incurred by S-Company for it.

- Block chain relation : Although, S-Company will probably use the K-Chain blockchain later on for stuff such as getting payed, but also for technical stuff pertaining to the Web Products. But use it, not pay for maintaining its codebase.

S-Company Initial Team Plans

Team Plans with money:

- Distributed team world wide.

- Paid in FIAT, or in crypto where acceptable / possible.

The Value

Key aspects:

- Only **product solution truly offering secure encryption**. No other suite so far. None. Nada.

  + Think also like Stuxnext, explosions in Teheran, etc.

- **Strategic value** from SKREM Suite applications

  + Think Telegram, WhatsApp, Facebook

- **First mover advantage**

- **Monetization options exist outside buyout**: charge for professional use, charge companies and organizations (modeled after GDL).

- For buyout, main value comes from:

  * Strategic Advantage

  * Denying similar capabilities to others and securing them for oneself

  * Licensing Product at much higher cost, leveraging corporate / govt / etc. entrances allowing such products to be bought.

The Value

- BTC non-zero addresses: 45 million. Overall estimate of people involved with crypto: 100 million worldwide (including for just momentary transfers). With market size 10% that's like 10 million people. At $250 each, that's **$0.25 billion** just for storing and using private keys to crypto.

- Adding journalists, enthusiasts and other categories, and considering repeat buys, just from SKREM-Suite Phase III probably its about **$1 billion in value to charge**, at **10% adoption rate**.

- Strategic value for **companies, organizations and gov't** is much higher..

- **Potential buyout will be $10-$100 billion**, depending on when, by whom and how. Out of that at least like $5-$25 billion will be "non-recyled", so for the S-Company stakeholders alone.

- If no **buyout, direct monetization possible**.

- Buyout terms will include that the suite to remains secure, available for personal use and open-source.

- Exit / Payback / Profit moments, unclear.. but costs expected to drop drastically in like 3 years. So "the moment of truth" is no more than 3-4 years ahead. After that probably another 2-3 years (or maybe 2-3 days) to start getting in large revenue streams or buyout courtship.

The Value: Indicators

- So, assuming full funding, this is like **a 5 year project for about $5 billion Total Lifetime Value**.

- To get everything done, done. And available online, and promoted for like 3-5 years and everything, probably like **$30-$50 millions is the max required** (with promotion a large portion of that).

- To get to Phase III technically, and do some minor online promotion, like first step, **I am seeking $10 million**.

The Value: $1Trillion Dollar Company?

- Can S-Company grow into a trillion dollar company as is? Probably not. NorthVPN company is valued at $3 billion. SKREM will probably exceed that, but reach like $100 billion, around there.

- **It *might* very well reach 1 trillion $$$ threshold if** we later diversify into full OS/Security/Encryption suite: basically dethroning Microsoft from "root OS" and having everyone use SKREM OS instead, with SKREM Suite and stuff installed by default.

- Actually, **it can also reach 1 trillion $$$ valuation in combination with R-Company** (the one operating the WebSuite part of the applications of SKREM Suite): that's strategic for global companies and customers, including business, gov't, dissidents and everyone.

- Also **it can reach 1 trillion $$$ valuation if it starts getting and doing contracts for govts** very heavily.

- Finally **it can reach 1 trillion $$$ valuation if someone pays like $100 billion for 10%** of the company, maybe 50% of that in own shares.. that can happen in a major buyout or via listing.

- Downside: If completed successfully, S-Company is expected to have at least like a few tens to hundred thousands customers per year after the first few years. So at 25,000 customers for $250 each (assuming no organizations), its like $6,250,000 per year - so both sustainable and able to payback original investment under the most sumbre scenario..

- Sumber scenario: Actually, the worst case is everything is developed, ready, promoted, but no one or very few actually buy it, no one is interested to further invest/buyout or purchase for strategic sectors. Then all investment is lost: well.. not lost.. it will have bought open source SKREM Suite to the World. But financially.

The Founder: Introducing Mircea Digulescu

Mircea Digulescu is a Leader, an Anti-imperialistic Libertarian Social Activist, an Independent Entrepreneur, Computer Science Researcher, Software Engineer, Military and Intelligence Enthusiast and Amateur Writer.

- See https://www.matsoft.ro/ for details on him in all these regards.
- Did found a $1.5 million company MAT SOFT TECHNOLOGY in 2009 (raised $300k from 3F) and later sold it in 2014.
- Speaks Russian, English and German fluently.
- Activist, politically opiniated and activist: libertarian ("good 1789 communist").
- Published peer-reviewed papers in Computer Science: https://www.matsoft.ro/Matsoft__Research62__Computer_Science_113.html.
- PhD (ABD - All but Dissertation) in Applied Computer Science from FMI UniBuc Bucharest.
- Professional Diploma in Management and B820 - International Strategy from OUBS (Milton Keynes).
- Lobachevky SU (1 semester, 2019), Nizhny Novgorod.
- Accepted but did not attend: SKOLKOVO Moscow School of Management (2013) and Cornell University (2004).

The Founder: Introducing Mircea Digulescu

Reached Div1 Coder on Codeforces.com (2022 max score): profile mircea85.

Built up Bolt.eu (Taxify)'s Bucharest Software Engineering office 2018/19 with Google experienced SSEs.

Had leadership roles (Team Lead, Manager)

Did presales.

Did very briefly LATOKEN crypto.

Socializes with diplomats and state bodies (Russia, China, Venezuela, Iran) and has political activity.

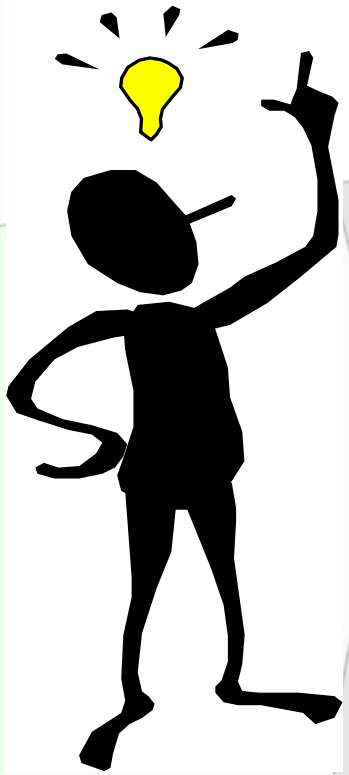
Was guest of Bolivarian Government in 2020 and promoted political speech in Caracas.

Is frequently visited by security services from accross.. when they learn about his wareabouts.

Was visited by CIA and whole of AUKUS in Germany in 2022.

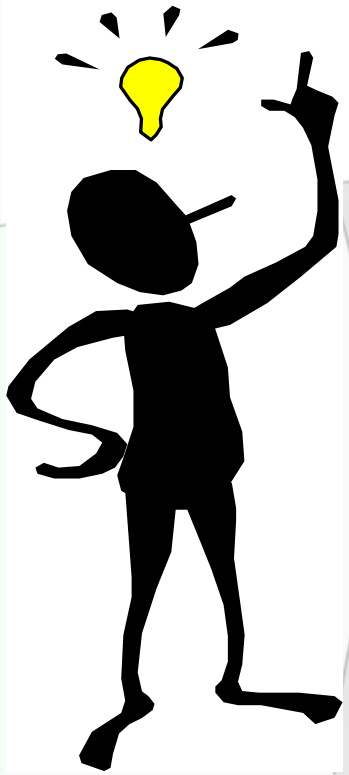
Got Assanged 2 days later and barely managed to escape with his life and unharmed in 2023. Barely, but did manage, so he is "alive and kicking" and will even more vigurously complete his projects.

S-Company: The Plan



- Build Phase I myself
- Put online
- Hire some team and contractors for Phase II and Phase III
- Hire non-technical people and do partnerships
- Experiment with best variant of SKREM
- Maybe do some Automatic SAT Solver test on simplified versions of SKREM to see how they fare
- Publish first MVP
- Get external paid audit of SKREM Suite
- Address any findings
- Complete full MVP and release publicly
- Massive promotion and advertising, partnerships
- Keep it up like 1-2 years
- Rip benefits
- Potential exit: partial buyout, major Round C investment, public listing, private listing, etc.

S-Company: The Deal



- You give money. I seek to raise $10 million in seed phase. If all goes well, probably another $25-$50 million in as Round A, and maybe $50 million Round B*

* Round B may not be required since S-Company (with K- and R- Companies) may become financially self-sufficient by then.

- $1 million should cover my plan up to "Publish first MVP" inclusively, so about 1-2 years. This includes upfront setup fees, etc.

- What do you get back?

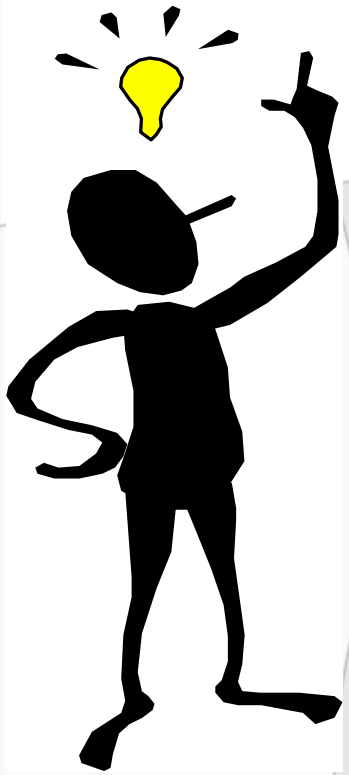
* You make SKREM Suite and S-Company happen (and via it probably K- and F-Companies also)

* The S-Company products will be available to the world, so including to you

* Something like 3-4% of S-Company.. Maybe a bit more.

* I am willing to put it in writing, but no funny legaleze. Best guarantee of you getting 3-4% if my undertaking to respect it. As the company grows, for Round A ($25-$50 million) there will probably be more paperwork and include stuff like IP and so on.

S-Company: The Deal



- How do you get it?

* Now that is hard.. if you choose to invest/donate/buy in BTC, you have by committal and undertaking that I will direct the 3-4% of company worth to you, on any capital event (of your choice) and of annual revenue (which will probably hopefully also be in BTC). IF ANY OF THESE SHOULD EVER HAPPEN. Your capital is at risk. This is not investment advice. This is not an ICO nor IPO. Consider it a donation with no prospect of return.

* If you want some paper stuff for your $1 million, I will be happy to set up an entity in like Russia or UAE and give you 3-4% of it. But for $1 million, the licensing of IP will be much laxer: meaning basically I will also retain IP on myself as physical person - at least until the entity will become worth like $100 million or $1 billion.

* Open to discussion

- What more?

* I'll keep you updated on how it goes

* We'll even chat once in a while to sync and do stuffs

S-Company: The Deal

- What WON'T you get for the $1-$10 million?

  * I will not reduce the security of SKREM Suite

  * I will not abandon the idea nor its implementation

  * I will not introduce backdoors

  * I will not give control of the company/entity to you

  * I will not give brand to you

  * This kind of stuff which is maybe common for just Pre-Seed or Seed.

- Anything else?

 * Once SKREM Suite is a factual reality, then K-Company and R-Company start to make sense.

 * R-Company can easily become the next StarLink / Telegram / etc.

 * K-Company will maintain the K-Chain. This chain will be designed so that it gives some value to the founder's address (me). Some benefits can be shared with K-Company stakeholders.

 * Both R- and K- companies are possible once S-Company is a reality. So further investment/donation opportunities exist. Taken together, the S-, K-, R-, E- and F- Companies, and thus the M-Company holding group definitely have the potential to become yet another major corporation, bigger than Uber, with major tech ramifications. This means $1 trillion dollar company, yeah.. and it all starts with S-Company. Warning: It can also all just fizzle miserably, so your capital is at risk. Consider anything sent/invested/donated/paid as certain losses. This is not investment advice.

MAT SOFT

Conclusions: S-Company in brief

- Solves a real problem (full e2e encryption): something others won't / can't.
- Leverages technical innovations by Mircea Digulescu: SKREM-like ciphers and their applications, security and web protocols, etc.
- Can be monetized without buyout: ~ $6million per annum expected worst case scenario unless fizzle.
- Will be worth and valued at like $10-$100 billion.
- Offers strategic advantage to its controller

The Deal

1. You invest/buy/donate about $10 million upfront, for Stage 1. In like 2 years, another $25-$50 million is raised.
2. In circa 5 years the project is complete: the moment of truth. In circa 7-9 years the ripping of benefits enters full scale mode.
3. In circa 10 years exit opportunities and valuations of >$10 billion.
4. Will support other group companies like K-Company and R-Company with products and strategically. Together SKREMF-Companies can be end up being valued $1 trillion.
5. Can also fail miserably. Your capital is at risk. Consider any money donated/sent/invested as full lost. There are no refunds. This is not investment advice.

110 over 70

Regarding any 110/70 questions on Mircea Digulescu:

- My blood pressure is 120 over 60.

MAT SOFT

Thanks for your consideration!

Contact Mircea Digulescu now at mircea.digulescu@mail.ru or via WhatsApp/Telegram/Viber at +40736.617.391, for investment, donations, technical details or anything!

Please consider Donating. It will be great if, instead of boot-strapping, support from smart donations such as by yourself could be leveraged. Please see **Contact Mircea** to donate: BTC and fiat transfers in RUB are accepted. A BTC donation of 100-200 USD will mean a lot to him and his activism. Especially if you were able to repeat the gesture once in a while.

To donate in use the following BTC address: **bc1qtgt8ctz3ffd95dwxux3wed6nlq3r5mhhzg98zp**.

bc1qtgt8ctz3ffd95dwxux3wed6nlq3r
5mhhzg98zp

To donate in RUB use the following MIR card number: **2202 2023 9828 3287**.

To donate in any other currency, please use an online service such as Telegram Wallet, Binance or others or make use of an offline exchange or BTC ATM machine, like for example cryptoatm.ro to donate in BTC to the address above.