Fwd: Sovrin Stewards: REMINDER Feedback due on Sovrin Governance Framework V2 — Stakeholder Review Draft 02 documents

-------- Forwarded Message --------

Subject: Re: Sovrin Stewards: REMINDER Feedback due on Sovrin Governance Framework V2 — Stakeholder Review Draft 02 documents
Date: Wed, 31 Oct 2018 10:45:51 -0600
From: Daniel Hardman <daniel.hardman@evernym.com>
Reply-To: daniel.hardman@evernym.com
To: Deventer, M.O. (Oskar) van <oskar.vandeventer@tno.nl>
CC: Markus Sabadello <markus@danubetech.com>, Nicolov, Kalin <Kalin.Nicolov@sicpa.com>, Peter L. Nohelty <Peter.Nohelty@rcu.org>, Dan Gisolfi <gisolfi@us.ibm.com>, Drummond Reed <drummond.reed@evernym.com>, adamg@us.ibm.com, Darrell O'Donnell <darrell.odonnell@continuumloop.com>, Elizabeth Renieris <elizabeth.renieris@evernym.com>, Heather Dahl <heather@sovrin.org>, Matt Norton <matt@sovrin.org>, Nathan George <nathan.george@sovrin.org>, Phil Windley <pjw@sovrin.org>, Riley Hughes <riley@sovrin.org>, Roy Avondet <roy@sovrin.org>, rtsulkin@michaelbest.com, Steve Fulling <steve@sovrin.org>, stewards@sovrin.org

Markus, thank you for patiently articulating your concern again. This is the first time that I have understood its tight connection to key management, as opposed to the more general issues of centralized communication or infrastructure.

I would like to discuss this further, now that I understand better, but I've already cluttered this particular thread in a way that abuses its subject line. I will start a new thread in the public TGB mailing list, with subject "avoiding centralization of validator and steward keys," in case anybody on this thread wants to join that side discussion.

--Daniel

On Wed, Oct 31, 2018 at 2:49 AM Deventer, M.O. (Oskar) van <oskar.vandeventer@tno.nl> wrote:

> Markus, all,
>
> Great discussion, touching some fundamentals.
>
> As mentioned, the first priority is transparency, detection the level of Cloud Provider “monoculture”.
>
> Note that the main risk may not be that a Cloud Provider or some of its key staff goes rogue, but that a rogue nation gives a secret order to subtly sabotage the system to a Cloud Provider that has its headquarters in that

nation. Sufficient jurisdictional diversity is hence needed for both Stewards and its supporting Cloud Providers, to assure that such a sabotage attempt does not go undetected.

Oskar

From: stewards@sovrin.org <stewards@sovrin.org> **On Behalf Of** Markus Sabadello
Sent: 31 October 2018 09:31
To: daniel.hardman@evernym.com; Nicolov, Kalin <Kalin.Nicolov@sicpa.com>
Cc: Peter L. Nohelty <Peter.Nohelty@rcu.org>; Dan Gisolfi <gisolfi@us.ibm.com>; Drummond Reed <drummond.reed@evernym.com>; adamg@us.ibm.com; Darrell O'Donnell <darrell.odonnell@continuumloop.com>; Elizabeth Renieris <elizabeth.renieris@evernym.com>; Heather Dahl <heather@sovrin.org>; Matt Norton <matt@sovrin.org>; Nathan George <nathan.george@sovrin.org>; Phil Windley <pjw@sovrin.org>; Riley Hughes <riley@sovrin.org>; Roy Avondet <roy@sovrin.org>; rtsulkin@michaelbest.com; Steve Fulling <steve@sovrin.org>; stewards@sovrin.org
Subject: Re: Sovrin Stewards: REMINDER Feedback due on Sovrin Governance Framework V2 — Stakeholder Review Draft 02 documents

Yes, many other factors (e.g. OS bugs) are much bigger and more immediate risks to the ledger.

There is just something very fundamental about this particular question where the validator keys are stored, it is those keys that together unlock the shared power over Sovrin's root of trust.
The very premise of distributed ledgers is to place this power in the hands of different people and organizations (as opposed to having a single central registry server).

Allowing one organization to hold multiple validator keys may not introduce high immediate risks, but it constitutes one small step directly against the basic foundational assumptions of why we're even building such a system in the first place.
A while ago another Steward asked me to host their node on their behalf, and I refused, convinced that the idea of one Steward hosting two nodes was completely incompatible with what the "Steward" role means.

To IBM's credit, they have themselves stated the following guideline:

"The Provider MUST NOT have access to the seed or private key of the Steward's Validator or Client. This prevents the Provider from being able to masquerade as the Steward, to subvert consensus, or to otherwise have more privileges than are absolutely necessary to function as a Provider."

But I don't see how this can be possible - IBM cannot credibly prevent itself from having access to the seed or key of a node that's running in its own IBM Cloud service.
To say that a Steward controls the validator keys on their IBM-hosted node is a bit like saying you control "your" profile on Facebook, or "your" files on Dropbox.

Those of us who have worked on decentralization for a long time and who feel the need for it in their hearts, must recognize that there's a basic contradiction here.
Decentralization and SSI are in many ways the antithesis to the "cloud" paradigm, and now that same paradigm is creeping back into the heart of this new identity architecture.

We can agree that the actual risk is very low (today!), for all the reasons you mention; and yes we can treat this as one risk of many, and yes the node selection algorithm can (perhaps) deal with it.
In some cases I even have sympathies for using a cloud provider, e.g. at IIW I spoke to one of the Stewards from a country where it's simply impossible to get local connectivity that is fast enough to be able to participate in the consensus protocol.

But still, allowing an organization like IBM to host multiple validator keys - especially if that organization is itself a Steward - feels like crossing a strange line.

Markus

On 10/29/18 11:23 PM, Daniel Hardman wrote:

> Markus:
>
> You have made this point eloquently and emphatically. I have argued back in several places.
>
> I think the reason we are not convincing one another is that we are not engaging on the same aspect of the problem. Let me explain why the metaphor of judge and jury doesn't move the needle for me, so that you can make a stronger case, if you feel inclined. I hope I really am not close-minded; I'm just needing different reasoning...
>
> I imagine that nearly 100% of the Board of Trustees, TGB, and Stewards of Sovrin uses a personal mobile device that's controlled by either Google or Apple. These are the mobile devices that we use to conduct official business; they could be tampered with by either company to interfere with the network in various ways. In theory.
>
> Nearly the same ratio applies to the duopoly of Intel and AMD -- almost all of our validator nodes and personal laptops/workstations run on chips made by the same 2 manufacturers. A lot of secrets pertaining to the operation of the network, including the keys of every steward, are probably stored on such hardware. All the source code is stored on such hardware. All our builds run on such hardware and are signed by such hardware.
>
> The relevant question, in my mind, is not whether concentration happens; it's *whether risk to network integrity changes, significantly and credibly, as a result of a particular concentration*. In other words, just because the jury has some common characteristic does NOT, in my mind, mean that it's likely that individual members will collude (either on their own or under the influence of some invisible manipulator). That's why we don't make noise about centralization on intel-compatible hardware; we just don't think that vector is very risky. Ruining Sovrin that way would be expensive and time-consuming, and would likely be found out.
>
> Now, guessing about risk is subjective. I totally admit that. And I could be guessing wrong.
>
> Having said that, I think the chances that a global hosting provider like {IBM, AWS, Azure, RackSpace, Google Cloud Engine, ...} would use its power [not that it COULD use its power] to bring about some network-undermining outcome, without being discovered, is quite low--even if a national government like the US sent a security letter demanding such behavior. Why?
>
> - Surveillance of the public ledger can be accomplished without cooperation from any hosting provider. There's good reason to believe it's possible today, regardless of how nodes are hosted. So IMO surveillance risk doesn't change meaningfully based on this policy, no matter what we decide.
> - Tampering in a sophisticated way would require an accurate model of the consensus protocol, running in parallel but at a faster rate of speed than the network itself, such that opportunistic substitutions of state/transactions could be made. Unless someone has invented a way to do this that I don't know about, this is highly unlikely, as it would require investment of tens of millions of dollars to match the

R&D in the network's consensus algorithm to date. It would also have to be based on academic literature that we don't know about. Even dumb and clumsy tampering (e.g., drop all transactions from a particular submitter) will be detected and cause enormous noise in the logs, unless a single party controls all (not just 51%) of the network.

- Hosting providers have no motive to tamper, and they have incredibly strong legal, PR, financial, and strategic reasons to host with integrity.
- Any operation like this would take significant time and resources, plus coordination and thus communication across multiple nodes scattered around the world, which increases the likelihood of detection.
- All hosting providers care about customer trust, understand that such a move would be deadly to their business if discovered, and run in tech circles that have pushed back vocally and repeatedly against attempts at government coercion. They have *not* been successful in every case of pushback--the surveillance state is clearly a thing that should give us nightmares, and the amount of data they've turned over makes me squirm--but they do appear to have held the line at requests for back doors that allow active tampering.
- Large multinational conglomerates are not as centralized and capable of cloak and dagger as we might think. They consist of legal entities incorporated in many places. They have to satisfy many legal jurisdictions. They leak information like a sieve. They have whistleblowers and auditors. They grant permissions to staff in complex ways, and usually not on a global basis. They send email over insecure channels. They work in different timezones and have trouble syncing up.
- Microledgers shift most of the interesting personal data off the public ledger, anyway. If I wanted to spy, that's where all the juicy secrets would be found.

Note that these are NOT claims that hosting providers won't get national security letters, that hosting providers are perfectly ethical, that hosting providers are incapable of fraud, etc. They are simply claims that this particular attack vector is not the one a rational attacker would prefer.

When I consider all of this, I think the chances that tampering (either instigated by a government, or instigated by evil corporate entities on their own) would undermine the network without detection are vanishingly small. I contrast this with the risk of Sovrin having a failed upgrade, of having a heartbleed-type OS vulnerability, of being shut down in a single legal jurisdiction, of natural disasters, of a denial-of-service attack, of poorly configured firewalls, of bugs in the software... and I feel surprised that we are giving the hosting provider risk any attention. All else being equal, I'd love diversity of hosting providers. But really, it doesn't feel very important, and pushing hard for it complicates politics and adoption. It's more likely to sink Sovrin from discord than from actual intrusion.

For me, the way to make a super strong argument in behalf of restricting hosting providers is to focus on probabilities. Not probabilities that something will be possible in theory (like a meteor strike)--but probabilities that it will actually happen.

On Mon, Oct 29, 2018 at 3:32 PM Nicolov, Kalin <Kalin.Nicolov@sicpa.com> wrote:

> Markus, all,
>
> Implying collusion on the part of the cloud provider, who **may potentially** corrupt the vote by voting on behalf of (or, rather misusing the keys of) the stewards hosting with them? That constitutes data breach and is criminal in multiple jurisdictions, to my knowledge. Let's also keep in mind the set of voting keys can be revoked which is a clear, and might I add instant, recourse.
>
> My suggestion is to explore the possibilities:

a) Markus is right, we get to see the day a cloud provider abuses their control to collude and vote on behalf of X steward: do we have way to fix? My understanding is yes (revoke);

b) We're over-engineering, attempting to imagine all possible outcomes. The cost of friction and heavier governance may not scale as intended – are we prepared for that, or prefer we keep on the back-burner?

Kind regards,
Kalin

Kalin Nicolov

Snr Manager Digital Evolution

Direct +41 21 627 6027

Mobile +41 78 609 8529

kalin.nicolov@sicpa.com

From: stewards@sovrin.org [mailto:stewards@sovrin.org] **On Behalf Of** Peter L. Nohelty
Sent: Monday, October 29, 2018 10:05 PM
To: 'Markus Sabadello' <markus@danubetech.com>; Dan Gisolfi <gisolfi@us.ibm.com>; =Drummond Reed <drummond.reed@evernym.com>
Cc: Adam M Gunther <adamg@us.ibm.com>; Darrell O'Donnell <darrell.odonnell@continuumloop.com>; Elizabeth Renieris <elizabeth.renieris@evernym.com>; Heather Dahl <heather@sovrin.org>; Matt Norton <matt@sovrin.org>; Nathan George <nathan.george@sovrin.org>; Phil Windley <pjw@sovrin.org>; Riley Hughes <riley@sovrin.org>; Roy Avondet <roy@sovrin.org>; Sulkin, Ryan T (35836) <rtsulkin@michaelbest.com>; Steve Fulling <steve@sovrin.org>; Stewards <stewards@sovrin.org>
Subject: RE: Sovrin Stewards: REMINDER Feedback due on Sovrin Governance Framework V2 — Stakeholder Review Draft 02 documents

Markus,

Another point of reference that we could look at is the VISA framework where their keys are stored for EMV cards. They are very prescriptive in how and where these keys are held and controlled (by the card processor or the financial institution). I think that I'm able to distribute these documents, but want to make sure there is interest before I send these document(s).

There also are other examples with ATM network and device encryption keys, signature and PIN pads used in bank and credit union branches and a host of other devices and systems that require storage and protection of keys in the financial industry. The use, control and storage of these keys are also examined by the regulators and vendors like VISA for compliance to their regulations and frameworks.

Hope some of these examples might be helpful.

Regards,

Pete

From: stewards@sovrin.org [mailto:stewards@sovrin.org] **On Behalf Of** Markus Sabadello
Sent: Monday, October 29, 2018 3:37 PM
To: Dan Gisolfi; =Drummond Reed
Cc: Adam M Gunther; Darrell O'Donnell; Elizabeth Renieris; Heather Dahl; Matt Norton; Nathan George; Phil Windley; Riley Hughes; Roy Avondet; Sulkin, Ryan T (35836); Steve Fulling; Stewards
Subject: Re: Sovrin Stewards: REMINDER Feedback due on Sovrin Governance Framework V2 — Stakeholder Review Draft 02 documents

CAUTION EXTERNAL ROYAL EMAIL
DO NOT open attachments or click on links from unknown senders or unexpected emails.

If a Steward uses IBM as a Hosting Provider, where are the Validator Keys stored?

I know you will say that the Validator Keys are protected by operating system configuration, geographical separation, business rules, legal protections, etc., but that doesn't change the simple fact that multiple Validator Keys will be stored in the IBM Cloud and could therefore be "controlled" by IBM.

You are correct that Danube Tech also uses a Hosting Provider - but no other Steward uses that same one.

Rather than comparing your Steward-as-a-Service offering to an Energy Provider, a more appropriate metaphor for the Sovrin pool would be that of a jury, where some of the votes are in the hands of the same judge.

Markus

On 10/29/18 3:26 PM, Dan Gisolfi wrote:

I agree with Markus this topic has been discuss at length.

Our position and approach is clear -- Cloud Providers are utilities not unlike Energy Providers.

Unlike the common practice in many countries where users do not have a choice of an Energy Provider, users (Stewards) do have a global choice for their Cloud Provider. But the Steward has a responsibility, as per the Steward Agreement, to the Sovrin Foundation.

The use of a Hosting Provider is common practice, even by Stewards like Markus in STFv1. In SGFv2 we have explicitly identified the persona of the Hosting Provider so that there can not and should not be any confusion where the lines of responsibility and risk are drawn.

IBM has advocated for a true SLA based Data Controller / Data Processor relationship when Hosting Providers are used in STGv2. This implies that the responsible entity remains the Data Controller (a.k.a. the Steward). Any Hosting Provider entering into such an arrangement should never, in our opinion, have access to or be in control of the Steward (Validator) Keys. That is just a basic design principle.

In our solution a Steward can hold us accountable for any malicious act by our employees. Contrast this to the pervasive practice of using arbitrary Cloud Providers today where the provider has zero stake in the network and the Steward has not taken any measures to mitigate the risk of their outsourced provider. Why is the community not concerned with this real issue?

We recognized the fact that Stewards, which do not host their own bare metal node and leverage a third party provider (which is the majority of Stewards today - including Markus), are at a greater risk of breaking the principles of our community then Stewards that rely on a Hosting Provider like IBM which is committed by legal instrument (an SLA or DPA with the Steward) to the requirements of the control documents.

Sadly in a community devoted to trust and transparency, we find push-back when community members desire to offer more restrictive and transparent solutions that mitigate the risks of the network.

DanG

From: "=Drummond Reed" <drummond.reed@evernym.com>

To: Markus Sabadello <markus@danubetech.com>

Cc: Stewards <stewards@sovrin.org>, Phil Windley <pjw@sovrin.org>, Heather Dahl <heather@sovrin.org>, Nathan George <nathan.george@sovrin.org>, Roy Avondet <roy@sovrin.org>, Steve Fulling <steve@sovrin.org>, Riley Hughes <riley@sovrin.org>, Matt Norton <matt@sovrin.org>, "Sulkin, Ryan T (35836)" <rtsulkin@michaelbest.com>, Elizabeth Renieris <elizabeth.renieris@evernym.com>, "Darrell O'Donnell" <darrell.odonnell@continuumloop.com>, Dan Gisolfi <gisolfi@us.ibm.com>, Adam M Gunther <adamg@us.ibm.com>

Date: 10/29/2018 04:59 AM

Subject: Re: Sovrin Stewards: REMINDER Feedback due on Sovrin Governance Framework V2 — Stakeholder Review Draft 02 documents

Markus,

From my understanding of the policies involved, there is a big difference between "hosting" and "controlling" a Sovrin steward node.

As far as I know, no one has proposed that a single organization have control—have access to the private keys—of more than one validator node.

But many stewards have chosen to host their node with a cloud provider, i.e., AWS, Azure, Google Cloud, etc. That cloud provider would not have access to the steward's private keys. As long as not too many stewards choose to use a particular cloud provider, do you see any issue with that?

From my understanding, all IBM is doing is creating a cloud hosting offering optimized for Sovrin stewards, but otherwise no different than hosting with a cloud provider that does not have such a specialized offering. I'm cc'ing Dan Gisolfi and Adam Gunther so they can confirm that.

Best,

=Drummond

On Mon, Oct 29, 2018 at 1:41 AM, Markus Sabadello <markus@danubetech.com> wrote:
I know the issue has already been discussed at length in various groups, but I want to state one more time that

1. I believe it is a big mistake by Sovrin Foundation to allow IBM (or any other organization) to host/control more than one validator node.
2. While I agree the node selection algorithm can in the future support the Diffuse Trust and High Availability principles, this particular issue is of special significance since it directly undermines the idea of a public distributed ledger.
3. Therefore the SGFV2 should explicitly prohibit any single organization from hosting/controlling more than one validator node.

Markus

On 10/27/18 2:58 AM, =Drummond Reed wrote:
Sovrin Stewards,

First, a huge thank-you to all the stewards who were able to attend the first All-Stewards Meeting last Monday prior to Internet Identity Workshop. It was highly productive to meet so many of you and be able to review and discuss shared issues and questions. And the interest in Sovrin at IIW the last 3 days was through the roof. The Sovrin credential demo given by the SF staff in attendance was so popular it had to be repeated all three days.

This is a reminder that **any additional feedback or comments on Stakeholder Review Draft 02 of the Sovrin Governance Framework V2 documents are due by next Monday Oct 29th**. The Sovrin Governance Framework Working Group has scheduled a special 2 hour meeting (beginning at 15:00 UTC in case anyone wants to attend—see details on the SGFWG Meeting Page) to review and ideally resolve any comments before preparing Public Review Draft 01 to submit to the Sovrin Board of Trustees for approval at their meeting on Oct 31.

See the email below for links to all 8 of the Google docs. Note that the four Policy docs altogether comprise less than 10 pages, so it does not need to take long to review and comment on them.

If you wish to make any comments privately, feel free to email them directly to me.

Thank you in advance,

=Drummond

On Sat, Oct 20, 2018 at 2:36 AM, =Drummond Reed <drummond.reed@evernym.com> wrote:
Stewards:

As promised on last Monday's All-Stewards call, below are the links to the **Stakeholder Review Draft 02** versions of all of the key documents in the **Sovrin Governance Framework V2** (formerly the Sovrin Trust Framework V2). For those of you traveling to the All-Stewards Meeting in Mountain View, CA on Oct 22, we hope this reaches you before you leave (note that these are all Google Docs, so if you wish to read them on a plane without wifi, remember to download PDF versions using the Google Doc File/Download As... menu before you take off).

Unlike Stakeholder Review Draft 01, which only included the three primary documents, Stakeholder Review Draft 02 includes **all four primary documents plus the Controlled Documents for SGF V2 policies** (those listed in section 5.3 of the Sovrin Governance Framework V2 document).

All of these are Google Docs that are now substantially complete and ready for detailed review and comments. Unfortunately due to the limitations of Google Docs (and the extent of some of the revisions), there is not a redline available (except for the Sovrin Steward Agreement, which you can request in Word format from Ryan). Here is the complete set of links:

1. **PRIMARY DOCUMENTS**

    1. Sovrin Steward Agreement Draft 04

    2. Sovrin Governance Framework V2

    3. Sovrin Glossary V2

    4. Sovrin Trust Assurance Framework V1

2. **CONTROLLED DOCUMENTS**

    1. Steward Business Policies

    2. Steward Technical Policies

    3. Sovrin Economic Policies

    4. Sovrin Trust Mark Policies

BEFORE REVIEWING/COMMENTING PLEASE READ THE FOLLOWING NOTES ABOUT EACH DOCUMENT:

Sovrin Steward Agreement Draft 04

This is a Google doc version of the same Word document that Ryan Sulkin sent out 10 days ago. **You may submit comments EITHER directly in this Google doc OR in the Word document version** that Ryan sent out on Oct 8 (and also attached to this email—note that Ryan's draft was not labeled Draft 04 but it is the same document). If you would like a redline against the previous version, contact Ryan (cc'd).

Sovrin Governance Framework V2

This document is now very mature and contains just a handful of action items. We urge you to carefully review the Core Principles and Core Policies.

Sovrin Glossary V2

This document is also very mature, now containing 190 glossary entries. A few key new terms are highlighted with comments. Note that it does not yet contain a handful of new entries coming from the Sovrin Trust Assurance Framework (below)—these will be added next week.

Sovrin Trust Assurance Framework V1

This document is new, as explained on last Monday's All-Stewards call. It is also relatively short and easy to understand.

Steward Business Policies

Very mature, and applies all stewards, so read closely.

Steward Technical Policies

Very mature, and applies all stewards, so read closely.

Sovrin Economic Policies

Although this document was originally for Sovrin token policies, however now that we have decoupled introduction of the Sovrin token from SGF V2, it is much simpler and should take only minutes to review.

Sovrin Trust Mark Policies

Once we added the Sovrin Trust Assurance Framework, we only needed this Controlled Document to state the basic policies for use of the Sovrin Trust Mark. Should take only minutes to review.

****
If you have any questions or general comments, feel free to email me (or the steward list) directly, or talk to me at the All-Stewards Meeting (or anytime during Internet Identity Workshop) in Mountain View next week.

Our goal is to produce Public Review Draft 01 by the end of the day on Monday Oct 29 and submit it to the Sovrin Board of Trustees for approval at their meeting on Oct 31, so please submit any comments by Sunday Oct 28 if possible.

Thank you,

=Drummond
Chair, Sovrin Trust Framework Working Group

RCU Confidentiality Notice: This email and any attachments, if applicable, are intended for only the addressee(s) named above. It contains information that is privileged, confidential, or otherwise protected from use and disclosure. If you are not an intended recipient, you are hereby notified that any review, disclosure, copying or dissemination of this transmission or taking of any action in reliance on its contents, or other use is strictly prohibited. If you have received this email in error, please notify us immediately by phone. Thank you for your cooperation.

The information in this email and any attachments is confidential and intended solely for the use of the individual(s) to whom it is addressed or otherwise directed. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Company. Finally, the recipient should check this email and any attachments for the presence of viruses. The Company accepts no liability for any damage caused by any virus transmitted by this email.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. TNO accepts no liability for the content of this e-mail, for the manner in which you use it and for damage of any kind resulting from the risks inherent to the electronic transmission of messages.