General Comments

In the few weeks I was engaged to work on servicing *MOBILITY PKI* requirements I had very limited access to PKI services in their broader sense - indeed no access whatsoever to production or pre-production environments. My sole environment used for any evaluation / validation was something called 'PDXXR.local' in NLP. I have not had access to design documentation other than an LTM, which I believe is intended as a substitute for what I would have known as a 'design'. I consider the LTM not to be fit for purpose as a design document. I have only seen a single 'installation guide', namely the "MSSSTP PKI - Low Assurance CA Commissioning Script v1.docx". I made 22 comments on the "Introduction" section of the document! A number of these comments related to simple inaccuracies, however, some I considered to be significant. I passed my commented document to Andy Nerton for him to give his *steer*. In this note, I use the term '2P CA' to refer to the ABC Class 2 Primary CA.

The observations I make here are not comprehensive and may be inaccurate – given my limited access.

Observations

- All 2P CA autoenrolled certificates should be immediately revoked. All computers which are entitled to certificates will get new ones with *good CDPs*, and there'll be no legacy risks from wrongly enrolled certificates. MSSSTP should do this via a change so if it doesn't work as expected, everyone will understand the rationale for doing it (and it couldn't be validated in PP). I'd advise doing the revocation testing in PP first, but could understand going straight to production if there is was alternative approach realistically available
- HSM key protection for the 2P CA should be moved from OCS to module (as per my original design – the rationale for which was clearly described). Bryan has advised she would like this approach taken – but needs first to get PMA approval. I've tested 'private key protection migration' in PDXXR.local and put together a satisfactory KSC document which I've passed to Andy Nerton and Rab Lohan.
- Failover / DR design work – MSSSTP need proven and tested instructions, I'd need a significantly better understanding of Falcon / Budgie deployment (as well as a significant number of other areas) to do this properly. At the moment my Falcon / Budgie knowledge is limited to the fact that one is in Woking and the other is in Crawley and the following statement: in production there are four HSMs, two for Falcon and two for Budgie
- To my knowledge there are no DR / failover instructions or operational guides, I doubt there could be since the 2P CA has not been deployed pre-production where this would likely be fleshed out and validated
- DR methodology - SMTP notifications (to get the serial number of certificates issued since the last backup) should be deployed. In the implemented solution as is, MSSSTP can only recover to a certain point in time when the backup is taken – i.e. 11pm on any given day. A consequence of this approach is that any certificates issued prior to the 11pm backup are orphaned - i.e. cannot be revoked. In the context of stolen or lost laptops this is a significant deficiency - MSSSTP cannot revoke issued certificates, one of the few effective methods to prevent the wireless use is by terminating the computer account (if that is used during DA instantiation), otherwise a rogue laptop could be used for internet access with potentially embarrassing consequences. 'Unrevokable' certificates is a 'PKI sin' of high magnitude and likely to result in failure of an *assurance audit*.
- A new nShield Edge USB HSM has been purchased for a new *Reference* Root CA - I believe. I've enquired of Neil Watson regarding the whereabouts of a development laptop I worked with him on in Edinburgh House and was under his ownership; there was an nShield Edge USB HSM with the said laptop. I contacted Neil recently (as he is still in MSSSTP employ) and he advised me that PDXXR have the USB HSM in NLP - I have checked with a person who looks after a locked cupboard where it was supposedly kept – it is no longer present.
- PDXXR appears to have been instructed to take the CPS and CP as their 'PKI requirements' - this is a bad approach as those documents simply do not contain design requirements, they are more related to governance. PDXXR have seemingly focussed solely on technical delivery, which is the *easy bit* with PKI (certificates issued and CRLs published) - and not where its real value is. PKI shouldn't solely be considered to be a technical barrier - skilled hackers will, given enough time, overcome technical barriers; it's the promise of something implemented and operated with assurance and skilled / competent people that helps make PKI a suitable barrier to hostile parties
- Evaluate and refine the prescribed CDPs, ensure they are fit for purpose in each environment

- Perform a *PKI health check* on the 2P CA solution delivered in production. I'd need authority, i.e. rights to log onto equipment and look at it myself, to do this as I don't consider some of the responsible staff to be suitably trustworthy
- Develop proper operational instructions and implement role separation for production 2P CA
- Advise MSSSTP on how to perform a KSC - such as dealing with exception handling, and generally why it is done in such a way. The KSC I witnessed at Cobalt Square was not fit for purpose. *There was the ADCS backup fiasco, etc. And where did those backups to disk go to?* As a generalisation, I imagine MSSSTP needs a better understanding of who does what, and where, and why!
- Help Rob Logan (if he's PDXXR's chosen one) up to speed and mitigate the dependence upon existing CA support staff
- Advise / train PDXXR operators on what they are expected to be doing – and what the scope of the 2P CA is
- Understand and document CRL promulgation to the various CDPs - this is essential and a fundamental cornerstone of a robust PKI solution
- HSM software (and perhaps firmware) update in all environments – I would like to check if there's any kind of Thales insistence on only supporting recent versions - or at least firmware that's newer than seven years old. It's not too much a stretch of the imagination that in the event of an HSM failure, the first thing Thales would ask MSSSTP to do is get firmware updates applied – a difficult task in what would already be a *challenging situation*. I'd imagine MSSSTP are paying significant sums to Thales for Platinum support, it'd be nice to know it is actually valid. I'd like to review all Thales support contracts for suitability. I think a likely best case scenario is that Thales would indeed support MSSSTP in the event of an HSM failure, but would not accept risk.
- DR applies to the Root CA also (not just 2P CA) – it's not known if backups are taken now – they probably are, but I doubt there is certainty of how MSSSTP could utilise them for a failed Root CA. It only takes someone to drop the Root CA laptop resulting in a hardware failure, and the entire ABC PKI could be at risk of *unrecoverability*
- Author new LTMs and PTMs, the current documents I've seen are not fit for purpose – my understanding is that LTM is 'design', whereas PTM is 'install guide'
- Setup 2P CA monitoring tasks – instruct PDXXR support on what to look for. The entire *monitoring piece* needs a lot of attention.
- Advise STPO lead (if there is one – Andy Gom could be a suitable pick) on PKI services that are being implemented
- Work should be done on certificate profile and CPS documents until they are fit for purpose
- PKI deployments in Reference and PP should to be evaluated and made fit for purpose (if required)
- There should be a change of the mind-set of it being acceptable to deploy first into Production, then PP, then Reference!
- A comment made by someone about the DirectAccess client certificates needing to be published to AD has got me curious; I'm not saying it's wrong or MSSSTP shouldn't do it, I'm simply fascinated to see what purpose it serves.
- A typical use of 'publish certificate to AD' is for email encryption; that way an originator can encrypt a message with the recipient's public key (which could be obtained from the recipient's *email certificate* which might have been published to AD, and typically hence the GAL). Only the recipient (as the private key holder for the aforementioned email certificate) could decrypt the originator's message. In authentication / dig-sig scenarios, I can't think of a valid reason to publish certificates to AD. It's been inferred that it might help avoid a rogue client spoofing a legitimate DA client, but having the certificate published to AD doesn't mitigate this. Anyone / anything, in theory, who / which is domain joined could retrieve a domain published certificate. Typically, for authentication purposes, it is the use of the DA client's private key (by signing a snip of random data) and sending that signed snip to the edge device (relying party) where the real value is. It's a low priority, but it'd be useful to see documentation from the Cisco ACE edge box (or whatever) to learn its rationale for looking for a certificate's presence in AD
- Very minor quibble: it is suggested to leave certlog on C: as it makes DR a little bit simpler
- If I was to be tasked with the design and implementation of the 2P CA I'd be satisfied to be *on the hook* as someone who could recover the *Met PKI* following a disaster. However, with the 2P CA as it was commissioned with a flawed KSC and dubious backup confidence, etc. I could not give that assurance. I would be prepared to do a health check, but my endorsement may be limited as there may be many things I don't get adequate access to. MSSSTP should move beyond relying solely upon two staff, as it

presents an obvious risk – I don't believe "it's too hard / there is no one else" should be acceptable for MSSSTP.

Snippets of Task Profile Updates sent to Sean King and Andy Neilson

Review the results of Failover / DR stuff and make recommendations where appropriate

Rob Logan described to me the anticipated failover / DR network HSM approach and I consider it to be satisfactory. I've not had sight of any failover / DR documentation for the Class 2 HSMs or the Class 2 CA to review.

Co review the CDPs, ensure they are fit for purpose

The Class 2 CA CDPs in production are correctly designed and implemented, they are fit for purpose.

Review the PDXXR delivered operational instructions

I've not had sight of any Class 2 CA operational instructions to review.

Review the documented CRL promulgation to the various CDPs

I've not had sight of any Class 2 CA CRL promulgation documentation: either design, engineering or operational instructions; I am unable to make any comments.

Action Plan

I propose I perform a 2P CA health check next Wednesday and Thursday (two days) or next Tuesday, Wednesday and Thursday (three days), preferably engaging via j25. The deliverable would be a report and action plan for a way forward - I anticipate particular emphasis would likely fall upon DR. I imagine that 2P CA is probably in a fit state to issue certificates, but not to deal with any kind of failure / disaster recovery scenario, in a planned, comprehensive and assured manner. I don't see there is any capability to facilitate further solution development in PP, etc.

I strongly advise that none of the observations made by myself here are acted upon as I am not under contract and legal agreement with MSSSTP and therefore have no insurance liability cover.