The Truth About PKI

And How to Deal With it

Julian Ashbourn BSc (hons)

A Brief History

- PKI has been around for almost half a century
- It gained little traction as it was too complicated for most to implement and, for many, that remains the case
- The rise of the Internet and SSL certificates brought change
- It also brought many third party vendors into the picture
- Many organisations bought in tools to help with PKI
- They usually just added complication and cost
- Now, the situation has become even more complicated because of the use of the cloud

Automation

- The answer, according to most vendors, is automation
- However, this brings issues of its own and does not always work as expected
- The time and cost of setting up all of this automation often defeats the object
- It is cost which is never recovered by the host organisation
- It also erodes skills among the IT work force

Cloud Native

- The idea of ‘cloud native’ was flawed from the outset as there is absolutely no reason for it
- It has resulted in new development methodologies such as containers, ‘kubernetes’, sidecars, service meshes and more, all of which complicate things beyond belief
- The claimed benefit is that applications may be made live more quickly, but this is not a benefit
- The situation has further complicated the PKI situation

Load Balancing

- One claimed benefit of cloud native is that automated load balancing may take place, moving containers around among servers
- But this is occurring on the suppliers infrastructure and is therefore only of benefit to them
- This plays havoc with PKI and will result in an exponential rise in the number (and cost) of certificates
- Most developers do not have the skills to manage this situation

More Automation

- As a result of the cloud native debacle, PKI vendors are having to come up with their own automation systems
- This places the management of PKI further away from the host organisation, further eroding in-house skills
- This is a one way street, the return from which will be seen as impossible by many host organisations
- However, their PKI related costs will rise dramatically
- This could make their own operation uncompetitive

The Solution

- Avoid the cloud as much as possible
- Bring things back in-house and use your own infrastructure
- Use Open Source products everywhere you can, on every server and on the desktops as well
- Train your own IT staff and develop their Open Source skills
- Build and maintain your own in-house PKI
- Build and maintain your own web servers and manage the certificates accordingly

The Benefit

- There will be a cost to bringing things back in-house but this will be a once only cost and will be negligible compared to what would be paid to vendors within the same year
- You will have everything back under your own control
- All the software necessary is available at no cost whatsoever
- There will be no on-going licence fees
- The money saved by the organisation will be significant and savings may be passed on to consumers
- This is true for both public and private sectors

How to do it

- There exists a wealth of information among Open Source resources on-line
- This includes training in scripting languages, how to build certificate repositories, web servers and much more
- Information is also available to help manage self signed certificates as well as the integration of third party certificates
- This will be good for your IT staff who will, once again, become highly skilled

Further Help

- The book ‘PKI Implementation and Infrastructures’ published by CRC Press explains all of this, see;
- www.routledge.com
- https://julianashbourn.wordpress.com
- Or order from your local book shop