

A Brief History of Digital Certificate Use in the Government of BC.

Presented by: Riaz Bassari
Justice and Public Safety Sector



Way Back in Time

- In 2004, the Ministry of Justice and Attorney General identified a need to safeguard some of its information so it can be accessed by known users only.
- This was a problem with the existing technology and data administration model, where access control was not sufficiently fine-grained.

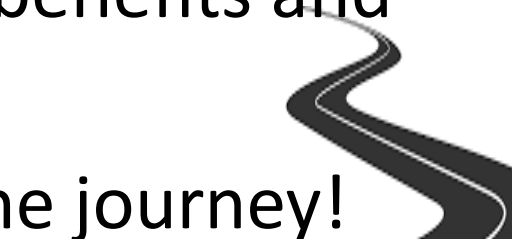
THEN

What We Had vs. What We Needed



- We had previously segregated our data in localized servers and set up firewalls around them to enhance access control.
- However, firewalls only filtered out computers, not unauthorized users on authorized computers...
- Share File and Print offered benefits but downgrading to simple operating system access controls was not acceptable.

Out Comes PKI

- Public Key Infrastructure and corresponding Digital Certificates could be used for data encryption, with access provided to named users only. - Hurray!
 - Second factor (in form of ikeys) would prevent unauthorized use, even in the event of userid and password breaches – Double Hurray!!
 - It also offered a number of other benefits and enhanced functionality,
 - So we committed to embark on the journey!
- 

The



First

- Terabytes of data were strongly encrypted and made accessible only to known users
- Data files were moved into shared storage space (cheaper) but remained completely secure.
- Each person was strongly authenticated with no chance of remote log-in by stolen credentials to access sensitive data, etc.

More Good News, for now



- Emails and attachments could be securely exchanged with other Digital Certificate holders in a seamless way.
- Digital Signatures were used to reduce paper and enable direct electronic approvals: Even Judges used Digital Signatures to finalize documents.
- Web based applications were put behind firewalls and accessed with a second factor, practically eliminating the chance of rogue access.

Reaping the Benefits

- All of this was put in place in 2005, and it is still in place to date.
- Our information security model has a new level of maturity, and
- Overall, we have more confidence in being able to handle and exchange highly sensitive material.



So What is the Bad News?



- It added cost and inconvenience:
 - Each person (over 800 of us) would need to be issued a Digital Certificate and an ikey with an initial cost and an ongoing maintenance fee.
 - Local Registration Authorities needed to be trained in each location to perform enrollments and password resets (re-enrollments)
 - IT staff needed to be trained for support of the new technology...



Change?

We Don't Need no Stinkin' Change!

- People didn't like the extra inconveniences:
 - At enrollment time, each person was required to authenticate themselves to an Local Registration Authority and present two pieces of ID !
 - If a password was forgotten, a form needed to be filled out, more ID presented and a wait of up to two days for a new Digital Certificate to be issued.
 - Each person needed to carry an small ikey to be inserted in the computer in order to access their files. And if they forgot it, they essentially couldn't work.

So We Managed Change

- We held face-to-face security awareness and training sessions,
- We educated everyone on the value of information security and their own individual responsibilities
- We all got to understand and accept that information security is sometimes inconvenient, but always necessary...
- And we bought and handed out chocolate. LOTS and LOTS of CHOCOLATE!



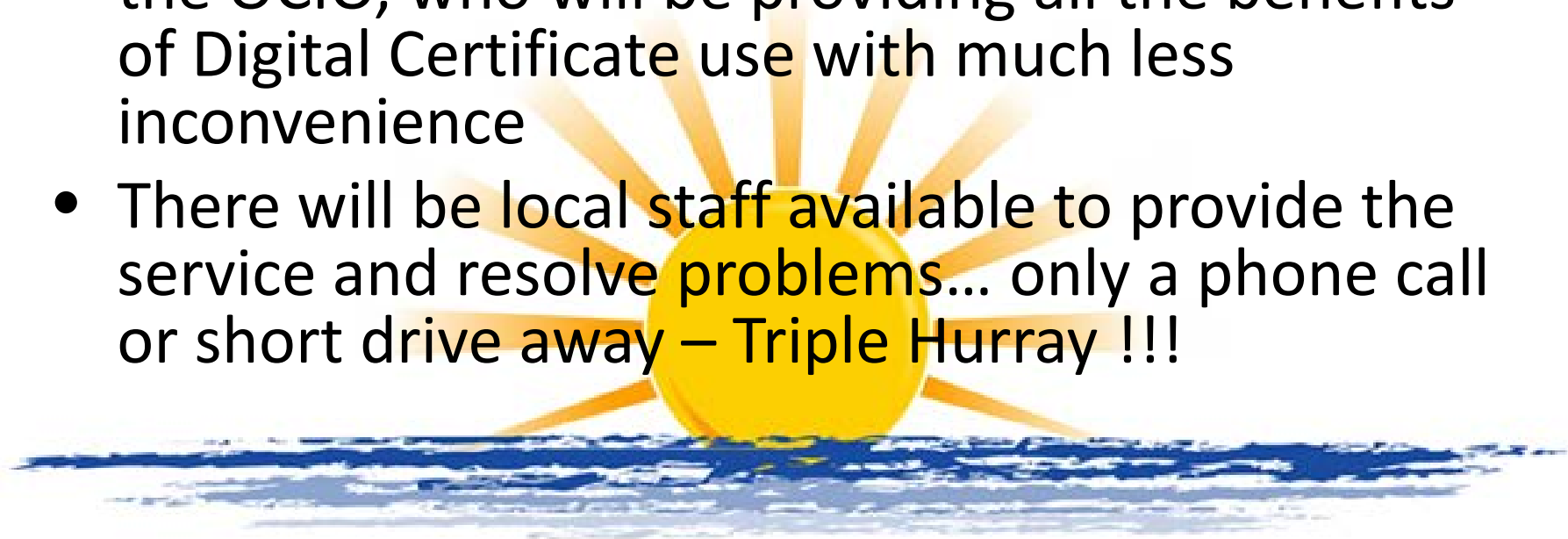
So Here We Are Today



- Our sensitive information is fully encrypted
- We can exchange secure (encrypted) emails and attachments (although only with other Digital Certificate holders)
- We authenticate ourselves with stronger controls to our systems and thus have more confidence in the confidentiality of information in our custody
- We can digitally sign emails and documents, giving the recipient more confidence in the authenticity of these.

All Thanks to Digital Certificates

- Historically, our Digital Certificate Service have been provided to us by the Federal Government, with a fair amount of necessary overhead and waiting periods in enrollments/reenrollments.
- Now, however, we have our own Digital Certificate Authority!
- the OCIO, who will be providing all the benefits of Digital Certificate use with much less inconvenience
- There will be local staff available to provide the service and resolve problems... only a phone call or short drive away – Triple Hurray !!!



In the Near Future

- **We are hoping that we can expand the use of Digital Certificates beyond strong authentication, encryption and non-repudiation. We could have:**
 - **Single Sign On,**
 - **Smart Cards,**
 - **Secure remote access,**
 - **Convenient and secure online financial transactions,**
 - **Perhaps an ID card that lets us in the building and gives us access to our workstations, applications and data,**
 - **Maybe our mobile phone will store our digital certificates and allow us to do all the above...**
 - **There are practically as many uses for Digital Certificates in information security as we can imagine.**

Wouldn't all that be nice?!

(Sales Pitch)

- Sign up now for our new DCS
- Get in touch with the OCIO and ask to be included in the next available time slot to have your ministry or organization equipped with the best information security an SLA can buy!
- **DON'T DELAY! CALL TODAY!**
- It's worth it!



Did everyone get Ken's contact information?

Thank You!

- Thank you for your time.

Questions?

Stay Safe and Secure!