Guión de Ceremonia de Claves DNSSEC de ABC

Abreviaturas

KMF= Instalaciones de Administración de Claves
TEB = Bolsa a prueba de manipulaciones o Bolas de Seguridad (bolsa grande DIEBOLD ítem #00051991000C bolsa pequeña #00051991000A)
HSM = Módulo de Seguridad de Hardware
FD = Memoria USB
SO = Oficial de la Seguridad
SA = Administrador del Sistema
SC = Controlador de la Caja Fuerte
IW= Testigo Interno
EW= Testigo Externo
MC= Maestro de Ceremonias
KSK= Key Signing Key
ZSK= Zone Signing Key
DVD del S/0 = DVD del Sistema Operativo
RNG= Generador de números aleatorios

Participantes

Instrucciones: Al final de la ceremonia, los participantes escriben su nombre, nacionalidad, firma, fecha, hora y el huso horario en la copia del SO.

Titulo	Nombre	Firma	Fecha	Hora
Ejemplo	Bert Smith	*Bert Smith*	12 Jul 2010	18:00 UTC
SA				
SO				
SC				
IW				
MC				
EW1				
EW2				
EW3				

Llegada de los Participantes

Paso	Actividad	Iniciales	Hora
1	El Administrador de Sistema (SA) escolta al Oficial de Seguridad (SO), al Controlador de Caja Fuerte (SC), al Testigo Interno (IW) y a otro personal autorizado hacia las instalaciones de Administración de Claves (KMF) después de que empiecen a filmar las cámaras.		

Registro para KMF

Paso	Actividad	Iniciales	Hora
2	El Administrador del Sistema (SA) registra a los participantes en el registro de las Instalaciones de Administración de Claves (KMF).		

Procedimiento de Evacuación de Emergencia

Paso	Actividad	Iniciales	Hora
3	El administrador de sistemas (SA) repasa el procedimiento de evacuación de emergencia		

Verifica Hora y Fecha

Paso	Actividad	Iniciales	Hora
4	El testigo interno (IW) escribe la fecha (mes/día/año) aqui, en tiempo UTC (Tiempo Universal Coordinado) de manera que todos tengan la misma hora razonablemente exacta de acuerdo al reloj visible en la pared: Fecha (UTC): _____ Tiempo (UTC): _____ Todos los procedimientos en este documento deberán seguir la hora UTC.		

Abrir la Caja Fuerte de las Instalaciones de Administración de Claves (KMF)

Paso	Actividad	Iniciales	Hora
5	El controlador de caja fuerte (SC), mientras cubre la combinación de la cámara, abre la caja fuerte.		
6	El controlador de caja fuerte (SC) toma el registro de la caja fuerte y escribe nombre, fecha, hora, firma, y motivo (Ej. 'Se abre la caja fuerte'). El Testigo Interno (IW) escribe sus iniciales en esta línea de registro.		

Remover el equipo de la caja fuerte de las instalaciones de Administración de Claves (KMF)

Paso	Actividad	Iniciales	Hora
7	El oficial de seguridad (SO) saca las tarjetas inteligentes (smartcards) en blanco (en una TEB) de la caja fuerte y llena en la siguiente casilla del registro de la caja fuerte, indicando el retiro como "Retiro de las Tarjetas Inteligentes," el numero de la bolsa a prueba de manipulaciones (TEB), nombre, fecha, hora impresas y la firma. El Testigo Interno (IW) escribe sus iniciales.		

Paso	Actividad	Iniciales	Hora
8	El administrador de sistemas (SA) saca el lector de tarjetas (en la TEB) de la caja fuerte y luego completa la siguiente entrada del registro indicando la retiro como “Retiro de lector de tarjetas,” el numero de la bolsa de seguridad (TEB), nombre, fecha, hora, y firma. Se ponen las iniciales del testigo interno (IW).		
9	El administrador de sistemas (SA) saca la bolsa de seguridad (TEB) con el DVD del S/O de la caja fuerte y completa la siguiente entrada del registro indicando el retiro como “Retiro de DVD,” el numero de la bolsa de seguridad (TEB), nombre, fecha, hora, y firma. El administrador de sistemas (SA) pone el ítem sobre la mesa de las instalaciones de Administración de Claves (KMF). El Testigo Interno (IW) pone sus iniciales.		
10	El administrador de sistemas (SA) saca de la bolsa de seguridad (TEB) HSMFD memorias USB en blanco, de la caja fuerte y completa la siguiente entrada del registro indicando el retiro como “Retiro del HSMFD.”, el numero de la bolsa de seguridad (TEB) nombre, fecha, hora, y firma. El administrador de sistemas (SA) pone el ítem sobre la mesa de las Instalaciones de Administración de Claves (KMF). El Testigo Interno (IW) pone sus iniciales.		
11	El administrador de sistemas (SA) saca la bolsa de seguridad (TEB) con la laptop de la caja fuerte y completa la siguiente entrada del registro indicando el retiro como “Retiro de Laptop,” el número de la bolsa seguridad (TEB), nombre, fecha, hora, y firma. El administrador de sistemas (SA) pone el ítem sobre la mesa de las Instalaciones de Administración de Claves (KMF). Se ponen las iniciales del testigo interno (IW).		
12	El administrador de sistemas (SA) saca cualquier unidad de poder, cables y otros equipos necesarios, de la caja fuerte y los pone sobre la mesa de las Instalaciones de Administración de Claves (KMF).		

Cerrar la Caja Fuerte de las Instalaciones de Administración de Claves (KMF)

Paso	Actividad	Iniciales	Hora
13	El controlador de la caja fuerte (SC) hace una entrada en el registro con el nombre, fecha, hora y firma indicando que se ha cerrado la caja fuerte. El Testigo Interno (IW) pone sus iniciales..		
14	El controlador de la caja fuerte (SC) pone el registro en la caja, la cierra y la bloquea.		
15	El oficial de seguridad (SO) y el administrador de sistemas (SA) verifican que la caja fuerte este cerrada.		

Establecer la Laptop

Paso	Actividad	Iniciales	Hora
16	El administrador de sistemas (SA) verifica la bolsa de seguridad (TEB) del DVD del S/O por evidencias de violación; lee el número de la bolsa de seguridad (TEB) mientras los participantes lo coinciden con la entrada del guión. TEB# 21094975		
17	El administrador de sistemas (SA) verifica la bolsa de seguridad (TEB) de la laptop por evidencias de violación; lee el numero de la bolsa de seguridad (TEB) mientras los participantes lo coinciden con la entrada del guión. TEB# 3112609		

Paso	Actividad	Iniciales	Hora
18	El administrador de sistemas (SA) saca el DVD del S/O y luego la laptop fuera de las bolsas de seguridad (TEBs), poniéndolos en la mesa de las Instalaciones de Administración de Claves (KMF); descarta las bolsas de seguridad (TEBs); conecta la laptop a la corriente, a la pantalla externa, a la impresora y arranca la laptop desde el DVD.		
20	El administrador de sistemas (SA) configura la pantalla externa para que los participantes vean.		
21	El administrador de sistemas (SA) se ingresa como "root".		
22	El administrador de sistemas (SA) configura la impresora y hace una impresión de prueba.		
23	El administrador de sistemas (SA) abre una ventana de la Terminal y lo maximiza para que los participantes vean (CTRL++).		
24	El administrador de sistemas (SA) abre una segunda ventana y ejecuta (Shift+Ctrl+F2): **sha256sum /dev/cdrom** Para verificar la autenticidad del DVD. El administrador de sistema (SA) puede continuar con otros elementos y luego vuelve a la ventana inicial. El sha256 hace para *"ICANN-DNSSEC-DEMO-20120925.iso"* debe ser: 0b347e56e9007d8fc269d440c6a008e8f6b09d687a1c74ffb22b349593d267b8		
25	El administrador de sistemas (SA) verifica la zona de tiempo, fecha, y hora en la laptop y la sincroniza si es necesario. Mostrar la hora y huso horario actual: **date** Si el huso horario no esta en UTC: **cd /etc/** **rm localtime** **ln -s /usr/share/zoneinfo/UTC localtime** Ajustar la hora al reloj de pared: **date mmddHHMMYYYY** Verificar: date		
26	El administrador de sistemas (SA) inspecciona la bolsa de seguridad (TEB) del HSMFD para verificar que no hayan evidencias de violación; lee el numero de la bolsa de seguridad (TEB) mientras los participantes lo coinciden con el guión principal. TEB# 19204938		
27	El administrador de sistemas (SA) saca el modulo de seguridad de hardware (HSMFD) fuera de la bolsa de seguridad (TEB); descarta la bolsa de seguridad (TEB); y lo conecta en una puerto libre de USB. El S/O debe reconocer el dispositivo USB (FD) como /media/HSMFD Si el FD no lo reconoce, El administrador de sistemas (SA) monta el modulo de seguridad de hardware (HSMFD) usando: **mkdir /media/HSMFD** **mount /dev/sda1 /media/HSMFD** Donde /dev/sda1 debe ser el dispositivo de USB (FD) en el dmesg. Luego presente en la pantalla a los participantes ls –lt /media/HSMFD		

Empezar a Registrar la Sesión de la Terminal

Paso	Actividad	Iniciales	Hora
28	El administrador de sistemas (SA) ejecuta: **`script /media/HSMFD/script-20121001.log`** para empezar una captura de la terminal.		

Conectando el lector de Tarjeta.

Paso	Actividad	Iniciales	Hora
29	El administrador de sistemas (SA) inspecciona y verifica la bolsa de seguridad (TEB) para que no haya evidencia de violación; lee el TEB# mientras los participantes lo coinciden con el guión principal. TEB# 21094976		
30	El administrador de sistemas (SA) remueve el lector de la bolsa de seguridad (TEB); descarta la bolsa de seguridad (TEB); y conecta el lector en un puerto libre de USB de la laptop.		

Iniciación las Tarjetas Inteligentes

Paso	Actividad	Iniciales	Hora
31	El oficial de seguridad (SO) verifica la bolsa de seguridad (TEB) de las tarjetas inteligentes para que no haya evidencia de violación; lee el numero de la bolsa de seguridad (TEB) mientras el administrador de sistema (SA) lo coincide con el guión principal. TEB# 3379422 Y saca la tarjeta inteligente de la bolsa de seguridad (TEB) y luego descarta la bolsa de seguridad (TEB).		
32	El oficial de seguridad (SO) saca una tarjeta y la conecta en el lector. La luz del lector debe parpadear.		
33	El oficial de seguridad (SO) inicia la tarjeta inteligente corriendo: carderase El oficial de seguridad (SO) ingresa un nuevo pin de 8 dígitos mientras lo cubre de la cámara. Si se reúsa una tarjeta previamente iniciada, puede preguntar por el el PIN del Oficial de Seguridad ("Security Officer PIN")., responda con el PIN previamente utilizado para esta tarjeta. Nota: Para nuestra configuración el PIN, PUK, y (SO) PIN son iguales.		
34	El oficial de seguridad (SO) ejecuta: cardshow para mostrar el contenido de la tarjeta.		

Iniciar el Generador de Números de Hardware (RNG)

Paso	Actividad	Iniciales	Hora
35	El administrador de sistema (SA) inicia el RNG abriendo una nueva ventana de la terminal y ejecutando: cardrng El oficial de seguridad (SO) escribe el PIN cuando sea pedido.		
36	El administrador de sistemas (SA) prueba el RNG regresando a la terminal y ejecutando:		

Paso	Actividad	Iniciales	Hora
	rngtest < /dev/random esperando al menos 10 segundos; luego presionando CTRL-C. El numero de pruebas con éxito debe sobrepasar y exceder a cualquier fallo. Durante la prueba, la ventana de RNG debe tener puntos indicando la alimentación de números al azar al kernel.		

Generar Nuevos ZSKs

Paso	Actividad	Iniciales	Hora
37	Para generar la ZSK en un disco RAM, el administrador de sistemas (SA) ejecuta: **export DOMAIN=py** **export TEST=yes** **genzsk** Note que la ventana de la tarjeta debe estar mostrando "…", indicando actividad. Los ZSKs públicos termina en .key. La mitad privada de los códigos encriptados termina en .private. El administrador de sistemas (SA) puede mostrar el directorio usando ls -lt		

Generar una Nueva KSK y Ponerlo en las Tarjetas-Inteligentes

Paso	Actividad	Inicial	Hora
38	Para generar el KSK en el disco RAM, El administrador de sistemas (SA) ejecuta: **genksk** y escribe "temp" como nombre del archivo.		
39	El administrador de sistemas (SA) pone la impresora estacionaria y ejecuta: **enscript --copies=N [-p out.ps] temp.out** y les entrega las copias a los participantes. "N" es el numero de copias.		
40	El administrador de sistemas (SA) lee la hilera de verificación de la llave presentada en la pantalla a los participantes mientras los mismos participantes lo coinciden con las impresiones para asegurarse de que los participantes se lleven con ellos la verificación de que el KSK que haya generado en esta ceremonia sea el mismo que se despliegue del DNS.		
41	El administrador de sistemas (SA) pregunta: "¿Alguno se opone?"		
42	El testigo interno (IW) adjunta una impresión de su guión la impresión.		
43	El administrador de sistemas (SA) detiene el RNG yendo a la terminal de RNG y presionando CTRL+C y saliendo de la ventana.		
44	El oficial de seguridad (SO) ejecuta: **cardwrite** y escribe "temp" para el archivo KSK, Kpy20121001 para CKA_LABEL, seguido del PIN cuando se deba poner el nuevo KSK en la tarjeta inteligente.		
45	El oficial de seguridad (SO) ejecuta: cardshow Para verifica los contenidos de esta tarjeta ya sean llaves privadas o publicas bajo la etiqueta Kpy20121001. El oficial de seguridad (SO) quita la tarjeta etiquetada con Kpy20121001, y la		

Paso	Actividad	Inicial	Hora
	etiqueta con la fecha y "KSK 1 de 3". El oficial de seguridad (SO) luego escribe la misma información junto con el nombre impreso y la firma en la nueva bolsa de seguridad (TEB) y pone la tarjeta dentro de la bolsa de seguridad (TEB). Finalmente el oficial de seguridad (OS) escribe el numero de la bolsa de seguridad (TEB) y CKA_LABEL aquí: Descripción: KSK 1 de 3 TEB# _____ CKA_LABEL Kpy20121001 El testigo interno (IW) pone las iniciales en la bolsa de seguridad (TEB).		
46	El oficial de seguridad (SO) toma una nueva tarjeta inteligente y la conecta en el lector. La luz del lector parpadea.		
47	El oficial de seguridad (SO) inicia la tarjeta ejecutando: carderase El oficial de seguridad (SO) escribe el mismo PIN mientras lo cubre.		
48	El oficial de seguridad (SO) corre: **cardwrite** y escribe "temp" para el archivo KSK, Kpy20121001 para CKA_LABEL y seguido del PIN cuando sea necesario escribir el nuevo KSK en la tarjeta.		
49	El oficial de seguridad (SO) luego ejecuta: cardshow Para verificar contenidos de la tarjeta para ver llaves privadas y publicas etiquetadas con Kpy20121001. El oficial de seguridad (SO) quita la tarjeta etiquetándola como Kpy20121001, fecha, y "KSK 2 de 3". El oficial de seguridad (SO) luego escribe la misma información junto con el nombre y la firma en la nueva bolsa de seguridad (TEB) y sella la bolsa de seguridad (TEB). Finalmente, el oficial de seguridad (SO) escribe el numero de la bolsa de seguridad (TEB) y CKA_LABEL aquí: Descripción: KSK 2 de 3 TEB# _____ CKA_LABEL Kpy20121001 El Testigo Interno (IW) pone sus iniciales en la bolsa de seguridad (TEB).		
50	El oficial de seguridad (OS) toma una nueva tarjeta y la conecta en el lector. La luz del lector debe parpadear		
51	El oficial de seguridad (OS) inicia la tarjeta ejecutándola como: carderase El oficial de seguridad (OS) pone el mismo PIN mientras se cubre de la cámara.		
52	El oficial de seguridad (OS) corre: **cardwrite** y pone "temp" para el archivo KSK, Kpy20121001 para CKA_LABEL, y seguidamente el PIN cuando sea necesario el nuevo KSK en la tarjeta.		
53	El oficial de seguridad (OS) luego ejecuta: cardshow Para verificar los contenidos de las llaves privadas y publicas etiquetada como Kpy20121001. El oficial de seguridad (OS) remueve la tarjeta etiquetada como Kpy20121001,		

Paso	Actividad	Inicial	Hora
	fecha, y "KSK 3 de 3". El oficial de seguridad (OS) luego escribe la misma información junto con la impresión del nombre y la firma en la nueva bolsa de seguridad (TEB) y lo pone en la mesa para usarlo luego. Finalmente el oficial de seguridad (OS) escribe el numero de la bolsa de seguridad (TEB) y CKA_LABEL aquí: Descripción: KSK 3 de 3 TEB# _____ CKA_LABEL Kpy20121001		

Borrar el Archivo de Llave Privado

Paso	Actividad	Iniciales	Hora
54	El administrador de sistemas (SA) borra la llave privada del disco RAM corriéndo: **shred -u temp** *Nota: Debido a técnicas de administración, no se puede ser garantizar el borrado de la memoria USB.		

- Generador de KSK Completado -

- Firmado de los RRset del DNSKEY -

Firmado del RRset del DNSKEY.

Paso	Actividad	Iniciales	Hora
55	El oficial de seguridad (OS) inserta la tarjeta KSK 3 of 3 en el lector y corre: **cardsign** CKA_LABEL es el valor usado arriba o Kpy20121001 Cuando se pregunte por el PIN, el oficial de seguridad (OS) lo pone mientras se cubre de la cámara. Esto generara RRsets (conjunto de registros de recursos DNS) firmados de la llave DNS (DNSKEY) y las llaves ZSK en archivos encriptados de la forma 20121001hhmmss.py.keybundle.tar.gz.aes256 al menos una susticion de ZSK		
56	El administrador de sistemas corre: **enscript --copies=N tt.dnskeyrrset.9** y entrega impresiones a los participantes para verificar que ZSK haya generado la misma hilera de verificación de la desplegada en el DNS dado en esta ceremonia. El DNSKEY RRset 9 tendrá las llaves publicas de ambas ZSK y de la próximo ciclo de sustitución (rollover).		
57	El testigo interno (IW) adjunta la impresión a su guión.		
58	El oficial de seguridad (OS) remueve la tarjeta inteligente del lector y lo pone en la bolsa de seguridad (TEB) "KSK 3 de 3" creada anteriormente, y la sella. El testigo interno (IW) pone sus iniciales en la bolsa de seguridad (TEB).		
59	El administrador de sistemas (SA) corre: **tar zcf /media/HSMFD/kc20121001.tar.gz .**		

Paso	Actividad	Iniciales	Hora
	Para archivar todo los resultados del ZSK+DNSKEY RRsets destinados por el registro y el DS para la zona superior.		

- Firma del DNSKEY RRset Completado-

Solo Para Demostración

Paso	Actividad	Iniciales	Hora
XX	El administrador de sistemas (SA) ejecuta: signzone Esto creara una zona de prueba, añade el DNSKEY RRset, descripta el ZSK de arriba. El administrador de sistemas (SA) puede poner en la pantalla todo el proceso de firmado usando: **`tail –f /tmp/namedb/signemd.out`** (para esta demo) o: **`monitor`** Para simplemente ver las llaves de ZSK y KSK usando “dig”.		

Terminar Registro de la Terminal

Paso	Actividad	Iniciales	Hora
60	El administrador de sistemas (SA) termina el registro de la terminal ejecutando “exit” en la ventana de la terminal		

Respaldar los Contenidos de HSM FD

Paso	Actividad	Iniciales	Hora
61	El administrador de sistemas (SA) muestra el contenido de la memoria USB del modulo de seguridad de hardware HSMFD ejecutando: **`ls –lt /media/HSMFD`**		
62	El administrador de sistemas (SA) conecta un modulo de seguridad de hardware HSMFD en blanco en la laptop, luego espera que lo reconozca el S/O como: /media/HSMFD_ y copia los contenidos de la HSMFD en una memoria USB en blanco para el respaldo ejecutando: **`cp -Rp /media/HSMFD/* /media/HSMFD_`** Nota: Solamente si los FDs no están preparados ni accesibles el administrador de sistemas (SA) seguirá los siguientes pasos para formatear y etiquetar: a) Conectar el FD b) Desmontar el FD (si se auto monta en el O/S) c) Determinar el nombre del dispositivo usando: dmesg (debe ser /dev/sdb1) d) Ejecutar mkfs.vfat –n HSMFD /dev/sdb1 e) Remover el FD		

Paso	Actividad	Iniciales	Hora
	f) Volver a insertar el FD y esperar para que el S/O lo reconozca.		
63	El administrador de sistemas (SA) muestra el contenido del HSMFD_ ejecutando: **`ls –lt /media/HSMFD_`**		
64	El administrador de sistemas (SA) desmonta el nuevo HSMFD usando: **`umount /media/HSMFD_`**		
65	El administrador de sistemas (SA) remueve el HSMFD_ y lo pone sobre la mesa.		
66	El administrador de sistemas (SA) repite los mismos pasos y hace 4 copias.		

Regresando el HSMFD hacia la TEB

Paso	Actividad	Iniciales	Hora
67	El administrador de sistemas (SA) desmonta el HSMFD ejecutando: **`umount /media/HSMFD`**		
68	El administrador de sistemas (SA) remueve el HSMFD y lo pone en la nueva bolsa de seguridad (TEB) y lo sella; lee el numero de la bolsa de seguridad (TEB); le muestra el ítem a los participantes y el testigo interno (IW) graba el numero aquí TEB # _____ Y lo pone sobre la mese de las Instalaciones de Administración de Claves (KMF).		

Regresando el O/S DVD hacia la TEB

Paso	Actividad	Iniciales	Hora
69	Después de que todos los trabajos de impresión estén completos, el administrador de sistemas (SA) ejecuta: **`shutdown –hP now`** remueve el DVD y apaga la laptop.		
70	El administrador de sistemas (SA) pone DVD en la nueva bolsa de seguridad (TEB) y la sella; lee el numero de la bolsa de seguridad (TEB) y enseña los ítems a los participantes y el testigo interno (IW) graba el numero de la TEB aquí: TEB# _____ Y lo pone sobre la mesa de las Instalaciones de Administración de Claves (KMF).		

Devolviendo la laptop en la TEB

Paso	Actividad	Iniciales	Hora
71	El administrador de sistemas (SA) desconecta el lector de tarjeta, la impresora, el monitor, y la fuente de poder, y toda otra conexión que este adherida a la laptop, seguidamente la pone sobre la bolsa de seguridad (TEB) y sella la bolsa; lee el numero de la bolsa de seguridad (TEB); muestra el ítem a los participantes y el testigo interno (IW) graba el numero de la bolsa de seguridad (TEB) aquí:		

Paso	Actividad	Iniciales	Hora
	TEB# _____ Y lo pone sobre la mesa de las Instalaciones de Administración de Claves KMF.		

Devolviendo el lector de tarjetas a la TEB

Paso	Actividad	Iniciales	Hora
72	El administrador de sistemas (SA) pone el lector dentro de la bolsa de seguridad (TEB) y la sella; lee en voz alta el numero de la bolsa de seguridad (TEB) y muestra el ítem a los participantes, el testigo interno (IW) graba el numero de la bolsa de seguridad (TEB) aquí: TEB# _____ Y pone la TEB sobre la mesa de las Instalaciones de Administración de Claves (KMF).		

Devolviendo los equipos de las TEBs a la caja fuerte de las Instalaciones de Administración de Claves (KMF).

Paso	Actividad	Iniciales	Hora
73	El controlador de la caja fuerte (SC) abre la caja fuerte cubriendo la combinación de la cámara.		
74	El controlador de la caja fuerte (SC) remueve de la caja fuerte el registro y lo llena con el nombre impreso, fecha, hora y firma indicando la abertura de la caja fuerte. El testigo interno (IW) pone sus iniciales.		
75	El oficial de seguridad (SO) graba el retorno de KSK 3 of 3 en el siguiente campo del registro con el numero de la TEB, nombre impreso, fecha, hora y firma. Pone los ítems en la caja fuerte. El testigo interno (IW) pone sus iniciales.		
76	El oficial de seguridad (SO) graba el retorno de KSK 2 of 3 en el siguiente campo del registro con el numero de la TEB, nombre impreso, fecha, hora y firma. Pone los ítems en la caja fuerte. El testigo interno (IW) pone sus iniciales.		
77	El oficial de seguridad (SO) graba el retorno de KSK 1 of 3 en el siguiente campo del registro con el numero de la TEB, nombre impreso, fecha, hora y firma. Pone los ítems en la caja fuerte. El testigo interno (IW) pone sus iniciales.		
78	El administrador de sistemas (SA) graba el retorno del lector de tarjetas en el siguiente campo del registro junto con el numero de la bolsa de seguridad (TEB), nombre impreso, fecha, hora y firma: pone el lector de tarjetas en la caja fuerte. El testigo interno (IW) pone sus iniciales.		
79	El administrador del sistema (SA) graba el retorno de la laptop en el siguiente campo del registro junto con el numero de la bolsa de seguridad (TEB), nombre impreso, fecha, hora y firma: pone la laptop en la caja fuerte. El testigo interno (IW) pone sus iniciales.		
80	El administrador del sistema (SA) graba el retorno del modulo de seguridad del hardware HSMFD en el siguiente campo del registro junto con el numero de la bolsa de seguridad (TEB), nombre impreso, fecha, hora y firma: pone el HSMFD en la caja fuerte. El testigo interno (IW) pone sus iniciales.		
81	El administrador del sistema (SA) graba el retorno del DVD del S/O en el siguiente campo del registro junto con el numero de la bolsa de seguridad		

Paso	Actividad	Iniciales	Hora
	(TEB), nombre impreso, fecha, hora y firma: pone el DVD del S/O en la caja fuerte. El testigo interno (IW) pone sus iniciales.		
82	El administrador del sistema (SA) regresa las Fuentes de poder, adaptadores y cables en la caja fuerte. No hace falta registro de esto.		

Cerrando la Caja Fuerte de las Instalaciones de Administración de Claves (KMF).

Paso	Actividad	Iniciales	Hora
83	El controlador de la caja fuerte (SC) hace una entrada para incluir el nombre impreso, la fecha, hora y firma, junto con notas al registro. El IW pone sus iniciales.		
84	El controlador de la caja fuerte (SC) pone el registro en la caja fuerte y la cierra.		
85	El oficial de seguridad (SO) y el administrador del sistema (SA) verifican que la caja fuerte este cerrada y bloqueada.		

Participantes firman el guión del testigo interno (IW)

Paso	Actividad	Iniciales	Hora
86	Todos los testigos externos (EWs) ponen el nombre impreso, fecha, hora y firma en el guión del testigo interno (IW).		
87	El administrador del sistema (SA), el controlador de la caja fuerte (SC) y el oficial de seguridad (SO(revisan el guión del testigo interno (IW) y lo firman.		

Desconectándose de las Instalaciones de Administración de Claves (KMF)

Paso	Actividad	Iniciales	Hora
88	El administrador del sistema (SA) se asegura que todos los participantes firman salida de las Instalaciones de Administración de Claves (KMF) y son escoltados afuera de las instalaciones.		

Se deja de filmar

Paso	Actividad	Iniciales	Hora
89	El administrador de sistemas (SA) deja de filmar con la cámara.		

Copiando y guardando el guión

Paso	Actividad	Iniciales	Hora
90	El testigo interno (IW) hace al menos 5 copias de su guión; uno para la auditoria exterior, otro para la auditoria interior, uno para el mismo, y copias para los participantes (según sea solicitado). Los bultos de las auditorias contienen 1) Un modulo de seguridad de hardware. 2) Copia del guión del testigo interno (IW) 3) Grabación audio-visual de la ceremonia 4) Una certificación del Administrador de Sistema (SA) y 5) Una certificación del testigo interno (IW) – Todo en una TEB etiquetada como “Ceremonia de Claves”, fechada y firmada por el testigo interno (IW) y por el administrador de sistema (SA). Uno de estos bultos		

Paso	Actividad	Iniciales	Hora
	será guardado por el administrador de sistemas (SA) en las Instalaciones de Administración de Claves (KMF) y el otro será guardado por el testigo interno (IW) en una caja fuerte de un banco.		

Todos los restantes participantes, son despachados de la ceremonia y desalojan la habitación.

Apéndice A.1:

Guión de la Ceremonia de la Llave

(por el testigo interno)

Por la presente certifico que la Ceremonia de la Llave en acuerdo con este guión y cualquier excepción que pudieron haber ocurrido fueron debidamente documentados.

Nombre Impreso: _____

Firma: _____

Fecha: _____

Apéndice A.2:

Revisión de la Configuración del Sistema del Control de Acceso

(por el administrador del sistema)

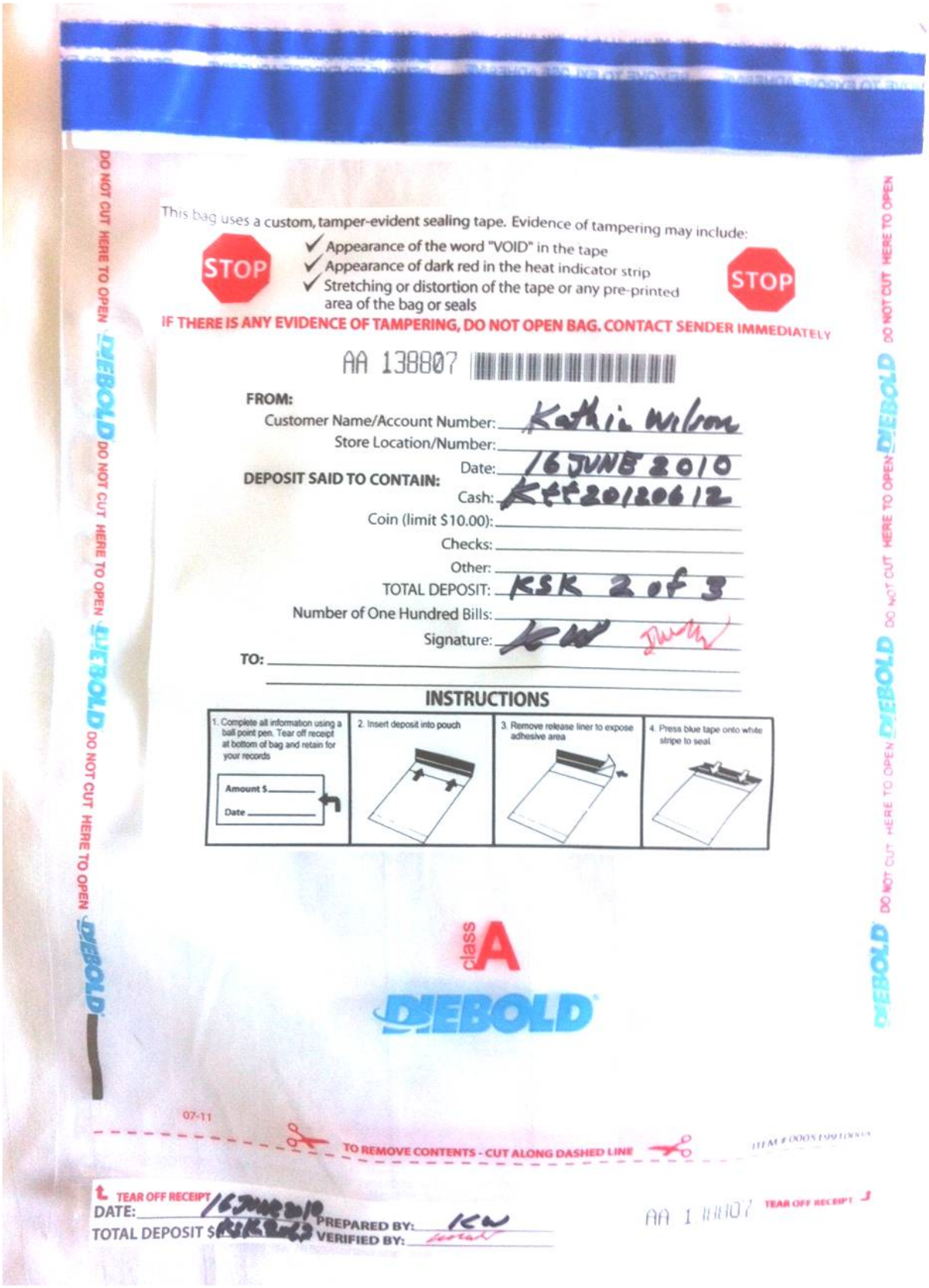
Por la presente certifico que he revisado físicamente el control de acceso al sistema y no encontré nada fuera de lo ordinario o que pudiese ser un problema.

Adjunto el registro físico del acceso

Nombre Impreso: _____

Firma: _____

Fecha: _____



This bag uses a custom, tamper-evident sealing tape. Evidence of tampering may include:

STOP

- ✓ Appearance of the word "VOID" in the tape
- ✓ Appearance of dark red in the heat indicator strip
- ✓ Stretching or distortion of the tape or any pre-printed area of the bag or seals

STOP

IF THERE IS ANY EVIDENCE OF TAMPERING, DO NOT OPEN BAG. CONTACT SENDER IMMEDIATELY

AA 138807

FROM:
Customer Name/Account Number: Kathi Wilson
Store Location/Number:
Date: 16 JUNE 2010

DEPOSIT SAID TO CONTAIN:
Cash: KSK20120612
Coin (limit $10.00):
Checks:
Other:
TOTAL DEPOSIT: KSK 2 of 3
Number of One Hundred Bills:
Signature: KW

TO:

INSTRUCTIONS

1. Complete all information using a ball point pen. Tear off receipt at bottom of bag and retain for your records
Amount $
Date
2. Insert deposit into pouch
3. Remove release liner to expose adhesive area
4. Press blue tape onto white stripe to seal

DO NOT CUT HERE TO OPEN DIEBOLD

class A

DIEBOLD

07-11

TO REMOVE CONTENTS - CUT ALONG DASHED LINE

TEAR OFF RECEIPT
DATE: 16 JUNE 2010
TOTAL DEPOSIT $ KSK 2 of 3
PREPARED BY: KW
VERIFIED BY:

AA 138807 TEAR OFF RECEIPT

A	Alfa	AL-FAH
B	Bravo	BRAH-VOH
C	Charlie	CHAR-LEE
D	Delta	DELL-TAH
E	Echo	ECK-OH
F	Foxtrot	FOKS-TROT
G	Golf	GOLF
H	Hotel	HOH-TEL
I	India	IN-DEE-AH
J	Juliet	JEW-LEE-ETT
K	Kilo	KEY-LOH
L	Lima	LEE-MAH
M	Mike	MIKE
N	November	NO-VEM-BER
O	Oscar	OSS-CAH
P	Papa	PAH-PAH
Q	Quebec	KEH-BECK
R	Romeo	ROW-ME-OH
S	Sierra	SEE-AIR-RAH
T	Tango	TANG-GO
U	Uniform	YOU-NEE-FORM
V	Victor	VIK-TAH
W	Whiskey	WISS-KEY
X	Xray	ECKS-RAY
Y	Yankee	YANG-KEY
Z	Zulu	ZOO-LOO
1	One	WUN
2	Two	TOO
3	Three	TREE
4	Four	FOW-ER
5	Five	FIFE
6	Six	SIX
7	Seven	SEV-EN
8	Eight	AIT
9	Nine	NIN-ER
0	Zero	ZEE-RO

Guión de Excepción de DNSSEC de ABC

Abreviaciones

TEB = Bolsa a prueba de manipulaciones
HSM = Modulo de seguridad del hardware
FD = Memoria USB
SO = Oficial de seguridad
IW = Testigo interno
EW= Testigo externo
SA = Administrador del Sistema
SC = Controlador de la caja fuerte

Instrucciones: Se ponen las iniciales del nombre en caso de llenar la nota, e.g., *BTS*. Notas para el tiempo.

Nota en caso de excepción del tiempo

Paso	Actividad	Iniciales	Hora
1	El testigo interno (IW) anota la fecha y la hora de alguna excepción de la Ceremonia de la Llave: _____		
2	El testigo interno (IW) describe la excepción.		

– Final del guión para la ceremonia del DNSSEC–