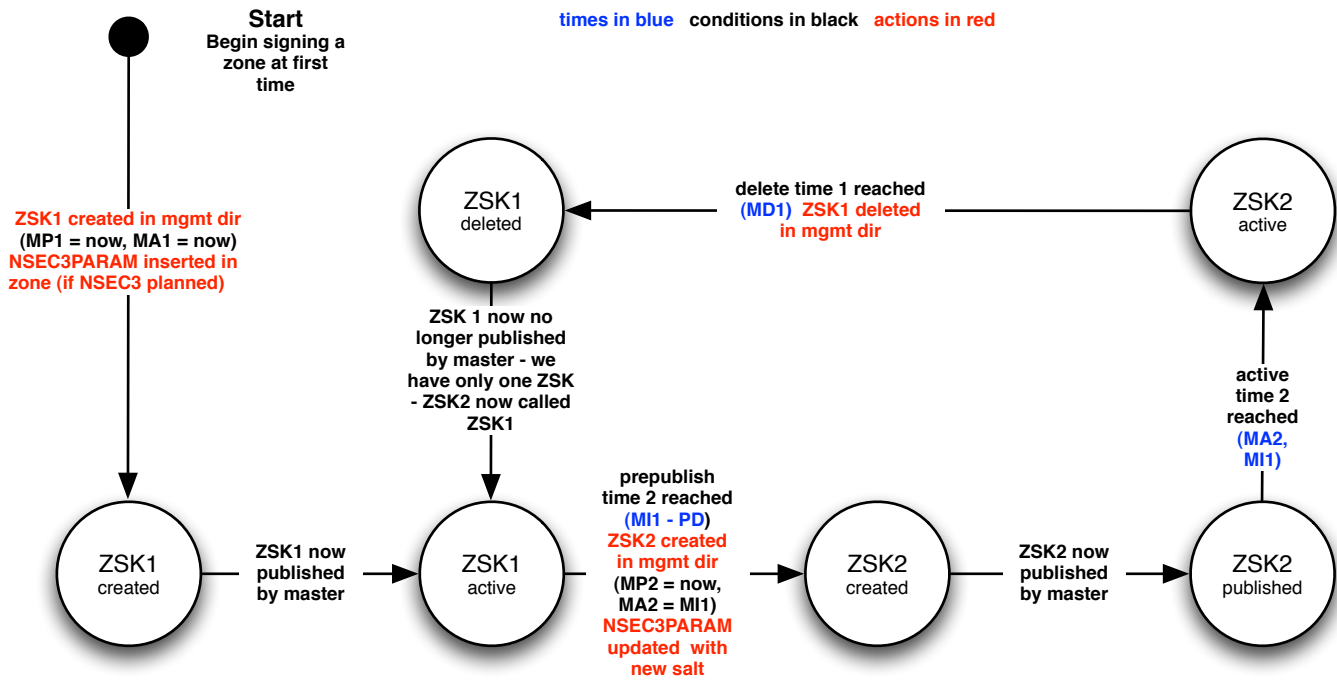**ZSK States (Pre-Publication-Method)**

Keys for Bind DNSKEY timing metadata triggering state transitions

MP — Date has passed, where key should be published to zone (publish)
MA — Date has passed, where named started using key for signing the zone (active)
MI — Date has passed, where named stopped using key for signing (inactive)
MD — Date has passed, where named stopped including key in zone (to be deleted)
MR — Revoke Date has passed (used to sign zone by bind with 'revoke' flag set)

PD — Propagation delay (time needed to reflect update in all caches) = prepublish time)
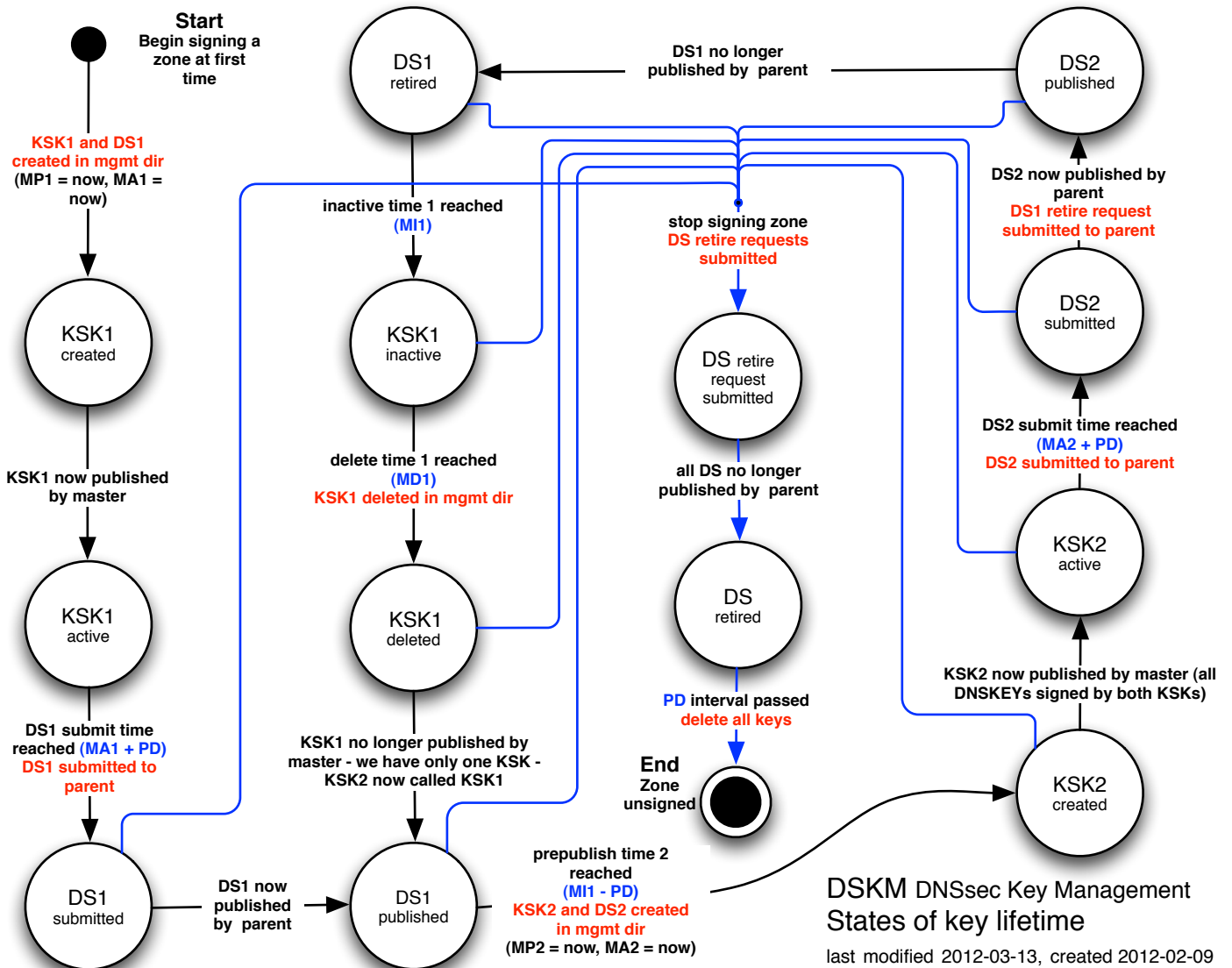
times in blue   **conditions in black**   **actions in red**

Start
Begin signing a zone at first time

ZSK1 created in mgmt dir
(MP1 = now, MA1 = now)
NSEC3PARAM inserted in zone (if NSEC3 planned)

ZSK1 deleted

delete time 1 reached
(MD1) ZSK1 deleted in mgmt dir

ZSK2 active

ZSK 1 now no longer published by master - we have only one ZSK - ZSK2 now called ZSK1

active time 2 reached
(MA2, MI1)

ZSK1 created

ZSK1 now published by master

ZSK1 active

prepublish time 2 reached
(MI1 - PD)
ZSK2 created in mgmt dir
(MP2 = now, MA2 = MI1)
NSEC3PARAM updated with new salt

ZSK2 created

ZSK2 now published by master

ZSK2 published

KSK States (Double RRSIG-Method ??)   (MD - MI) KSK > sig lifetime (1 week)

Start
Begin signing a zone at first time

KSK1 and DS1 created in mgmt dir
(MP1 = now, MA1 = now)

DS1 retired

DS1 no longer published by parent

DS2 published

KSK1 created

inactive time 1 reached
(MI1)

KSK1 inactive

stop signing zone
DS retire requests submitted

DS2 now published by parent
DS1 retire request submitted to parent

DS2 submitted

KSK1 now published by master

delete time 1 reached
(MD1)
KSK1 deleted in mgmt dir

KSK1 deleted

DS retire request submitted

all DS no longer published by parent

DS2 submit time reached
(MA2 + PD)
DS2 submitted to parent

KSK1 active

DS retired

KSK2 active

DS1 submit time reached (MA1 + PD)
DS1 submitted to parent

KSK1 no longer published by master - we have only one KSK - KSK2 now called KSK1

PD interval passed
delete all keys

KSK2 now published by master (all DNSKEYs signed by both KSKs)

End
Zone unsigned

DS1 submitted

DS1 now published by parent

DS1 published

prepublish time 2 reached
(MI1 - PD)
KSK2 and DS2 created in mgmt dir
(MP2 = now, MA2 = now)

KSK2 created

DSKM DNSsec Key Management
States of key lifetime

last modified 2012-03-13, created 2012-02-09
by: Axel.Rau@Chaos1.DE