BTNS API proposal overview

Michael Richardson
<mcr@xelerance.com>
Nicolas Williams
<Nicolas.Williams@sun.com>

IETF 69 - Chicago

Drafts are:

- draft-ietf-btns-abstract-api-00.txt
- some revisions this week already:
  - http://www.sandelman.ca/SSW/ietf/ipsec/btns/

Two objects

- pToken – “protection Token”
  - deals with details of one session (IPsec SA)
- iToken – what identity to use
  - translates to/from phase 1 ID
  - may include reference to credentials, such as from a smart card.

pToken attributes

- privacyProtected - boolean.
- integrityProtected - boolean.
- compressionAvailable - boolean.
- policyName - string. A handle which describes the system policy
  - "secure", "ospf", "iSCSI", "very-secure", "do-not-tell-mom-secure", "minimum-security",

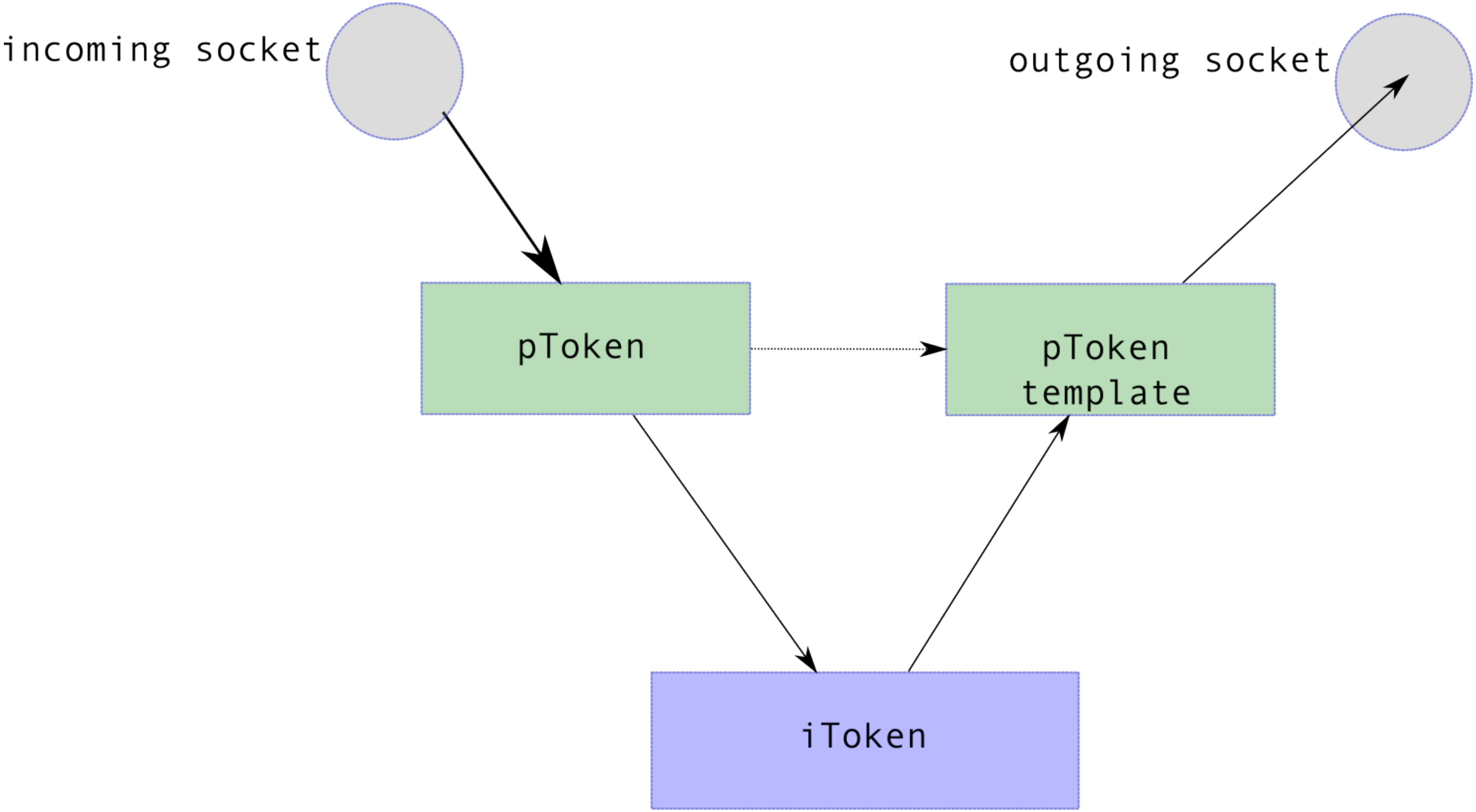
pToken attributes II

- iToken – object. me
- remote_iToken - object. them.
- tunnelMode – boolean.
- ipoptionsProtected - boolean. auditString - string.
- informationString - string.

iToken attributes

- auditString - string.
- authenticationMethod - enumerated type. (see text)
  - BTNS is one value.
- certificateAuthorityDN
- certificateDN – string.
- pubKeyID - string.
- channelBinding - binary blog.

Diagram of relations



incoming socket
outgoing socket
pToken
pToken template
iToken