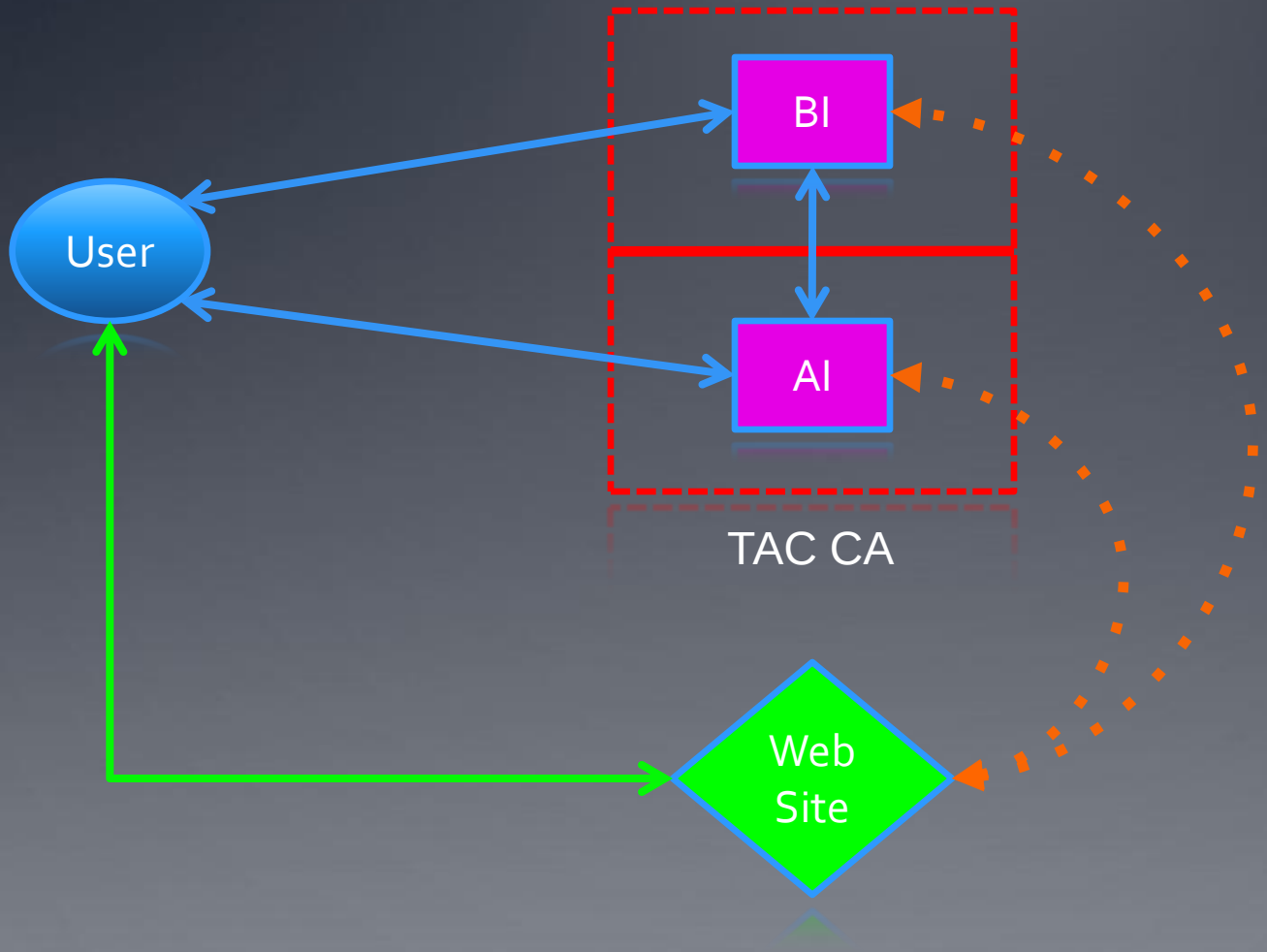
Traceable Anonymous Certificates Version 01 Revisions

Steve Kent (BBN) for SangHwan Park (KISA)

TAC Model



TAC Version 01 Revisions

- Jim Schaad provided extensive comments on the 00 version of the TAC internet draft
- This presentation reviews the changes made in response to Jim's comments
- For details see
  - My message of August 28
  - SangHwan Park's message of October 13
  - the 01 version of the I-D posted on October 28
- There has been no additional list traffic on this I-D, so I plan to issue WGLC soon, unless I hear otherwise

Responses (1/6)

- Certificate lifetime
  - The I-D will not mandate a lifetime, but it does call for the CP of the TAC CA to state the lifetime of TACs
- Scope for TAC use
  - The security considerations section now states that web access by users is the primary TAC context
- Who issues the CRL for TACs?
  - Issued by the AI, using a CA certificate restricted to CRL issuance, and with the same name as the TAC CA
  - This approach is not an indirect CRL as per 5280

Responses (2/6)

- TAC financial model
  - No model is specified; the I-D now recommends that the TAC CA offer only one lifetime for TACs
- TAC renewal/rekey problems
  - TACs will not be reissued or renewed
- Types of certificates issued by a TAC CA
  - A TAC CA will issue only EE certificates
- TAC CA retention of data
  - A TAC CA MUST state its data retention policy in its CP

Responses (3/6)

- Can a user request a pair of TAC certificates, one for encryption and one for signature?
  - The I-D now restricts TAC certificates to encryption only, consistent with the web access scope of TACs
- UserKey security
  - The I-D warns that the UserKey value MUST NOT be invertible to yield the user's real identity
- Confusion re certificates used with TLS and for CMS
  - The I-D has clarified that the certificates used for TLS are NOT used for CMS object signature validation

Responses (4/6)

- CRMF and PKCS #10 are not “protocols”
  - The I-D now refers to both as “formats” for conveying certificate requests and responses, and provides profiles for both in Appendices
- Against which threats is TLS providing protection?
  - The I-D now explains in more detail the security services required from TLS for each message exchange
- Certificate request/response may not be realtime
  - The I-D notes this and requires that the BI and AI use the Token and a database timeout scheme to accommodate interrupted certificate request processing

Responses (5/6)

- Make the Token a CMS ContentInfo object
  - Done
- Fix Figure 1 numbering of steps/arrows
  - Done
- Allow the BI to perform its own assessment of the abuse claim made by the aggrieved party, before releasing the true user identity
  - The text has been modified to allow the BI to perform an independent assessment, if the CP so states

Responses (6/6)

- Threshold crypto “fairness” between AI & BI
  - The scheme is independent of the specific threshold crypto algorithm, but we added text to note this concern, i.e., that neither BI nor AI should have an advantage in trying to determine the other’s key
- Is the spec clear enough on how to use TLS?
  - Appendix B has been added to try to clarify this, but we’ll have to see if the Application area ADs are satisfied