A Modular Public Key Infrastructure for Security Management

1. Key Escrow

Encryption in this PKI allows for any pair of registered usersto communicate securely provided they share a common cryptographic engine. When key escrow is mandatory, each user will be required to provide a copy of his secret encryption key(s) to one or more certified Escrow Agents (EA). When not mandatory, a user may choose to escrow his keys with a trusted third party or even act as his own Escrow Agent (in such a case split escrow may not offer any advantage).

In the following all arithmetic is done modulo a universal prime number p . Registering for encryption services requires:

- User A generates two secret numbers u_A and v_A
- User A escrows his secrets with the split Escrow Authorities E_1 and E_2 by generating two additional secret numbers u_1 and u_2 (which he must securely store for possible data recovery). Each Escrow Agent will have published a universal parameter g^{r_1} and g^{r_2} respectively, which allows User A to form the values $g^{r_1 u}$ and $g^{r_2 u_2}$. These values will be used to form keys to encrypt his secret information for sending to the Escrow Agents.
- User A sends tto his Escrow Agents:

$$A \rightarrow E_1 \colon \langle g^{u_1}, E^{u_1 r_1}(u_A), ID_{CA}, \ldots \rangle_A$$

$$A \rightarrow E_2 \colon \langle g^{u_2}, E^{u_2 r_2}(v_A), ID_{CA}, \ldots \rangle_A$$

  where E is a known, and fixed, encryption algorithm used by the Escrow Agents. The session key for the encryption is $g^{u_i r_i}$.
- Upon receipt, each Escrow Agent decrypts its part of the split secret, and computes g^{u_A} and g^{v_A}, respectively. Each archives the information sent by user A and sends back to User

~~FOR OFFICIAL USE ONLY~~

A's CA the package

$$\langle g^{u_A}, ID_A \rangle_{E_1}$$

$$\langle g^{v_A}, ID_A \rangle_{E_2}$$

respectively.

- Upon receipt of this information the CA is ready to register the user. It computes and forms the signed public key certificate

$$\langle \langle g^{u_A}, ID_A \rangle_{E_1}, \langle g^{v_A}, ID_A \rangle_{E_2}, ID_A, \ldots \rangle_{CA}$$

which it transmits to both User A (for verification) and to the Network Directory Server for placement in the public directory.

NOTES: A unique feature of this key escrow mechanism is that users must escrow their keys to get valid certificates. There is no way for the Certificate Authority to unilaterally enroll a user.

2. Encryption

Let us assume User B wishes to send User A a secure message. The following sequence is then followed:

- User B queries a Network Directory Server for User A's public key certificate.
- Upon receipt of User A's certificate User B computes a session key by forming

$$SK = H\left\{ H[H(g^{u_A u_B}, ID_B, ID_A, \text{month}),\text{day}] \oplus H[H(g^{v_A v_B}, ID_B, ID_A, \text{month}),\text{day}],\text{random} \right\}$$

where H is a commonly held hash function, the month field is eleven bits (allowing for 2048 possibilities in this proposal, but may be any length), the day is five bits, and the random field is at least forty bits (to avoid the same session key if many messages are sent by User B to User A on the same day).

- User B encrypts the signed message under the session key SK and sends to User A

$$\text{control bytes,month,day,random,}E^{SK}(\langle m \rangle_B)$$

where the *control bytes* indicate what encryption was used, the key lengths, and how to process the succeeding bytes. (User B might also send his public key certificate to avoid a network lookup by User A.) Alternatively, he may choose to use SK as a *key encryption* *key* (KEK) instead. In this case the message is encrypted with a random key, and an encrypted version of this random key is sent with the message. This latter encryption is performed under the session key.

- Upon receipt, User A computes the session key by forming $(g^{u_B})^{u_A}$ and $(g^{v_B})^{v_A}$. User A next decrypts the message and then authenticates it by checking that the signature is valid.

NOTES: The formula for session key is new. It allows for long term caching of the most computationally intensive part of the key. Thus, users who communicate often do not have to recompute the entire session key. The structure of the session key also allows for time bounded warrents for decryption. The only other scheme along these lines (Yacbi, Lenstra, Winkler) requires Users A and B to each send the other specific data, after which, on the third communication, the actual message is transmitted. We avoid these two exchanges.

3. Law Enforcement

The specific form of the session key allows for law enforcement to read traffic without explicitly being given either pair u_A, u_B or v_A, v_B. In particular, suppose a warrant is issued to read all the traffic sent by User B to User A during the month of March 1996. In terms of User A's Escrow Agents, the following sequence is then followed:

- User A's split Escrow Agents E_1 and E_2 are served the warrant.
- E_1 computes its half of the split key escrow u_A and sends to law enforcement (signed and encrypted):

$$E_1 \to \text{Law Enforcement: } \langle H(g^{u_A u_B}, ID_B, ID_A, \text{month}), ID_B, ID_A \rangle_{E_1}$$

- Similarly E_2 computes its half of the split key escrow v_A sends to law enforcement

$$E_2 \to \text{Law Enforcement: } \langle H(g^{v_A v_B}, ID_B, ID_A, \text{month}), ID_B, ID_A \rangle_{E_2}$$

- Each day law enforcement hashes the day field into each of these packets, adds them together, and hashes in the per message random field to generate a session key.

At this point law enforcement can read only that traffic specifically covered by the warrant. *No secret keys are revealed.* If the warrant covers a specific set of days, or even an extended period of time, the Escrow Agent generates several key packets that cover the specified time period. Similarly, key packets will have to be generated for each user and for each direction of transmission covered by the warrant. [redacted] [redacted] [redacted] Such circumstances should be extremely rare and governed by very stringent requirements.

(b)(1)
OGA

FBI

Once the warrant expires, the user has no need to generate new [redacted]

DRAFT

(b)(1)
OGA

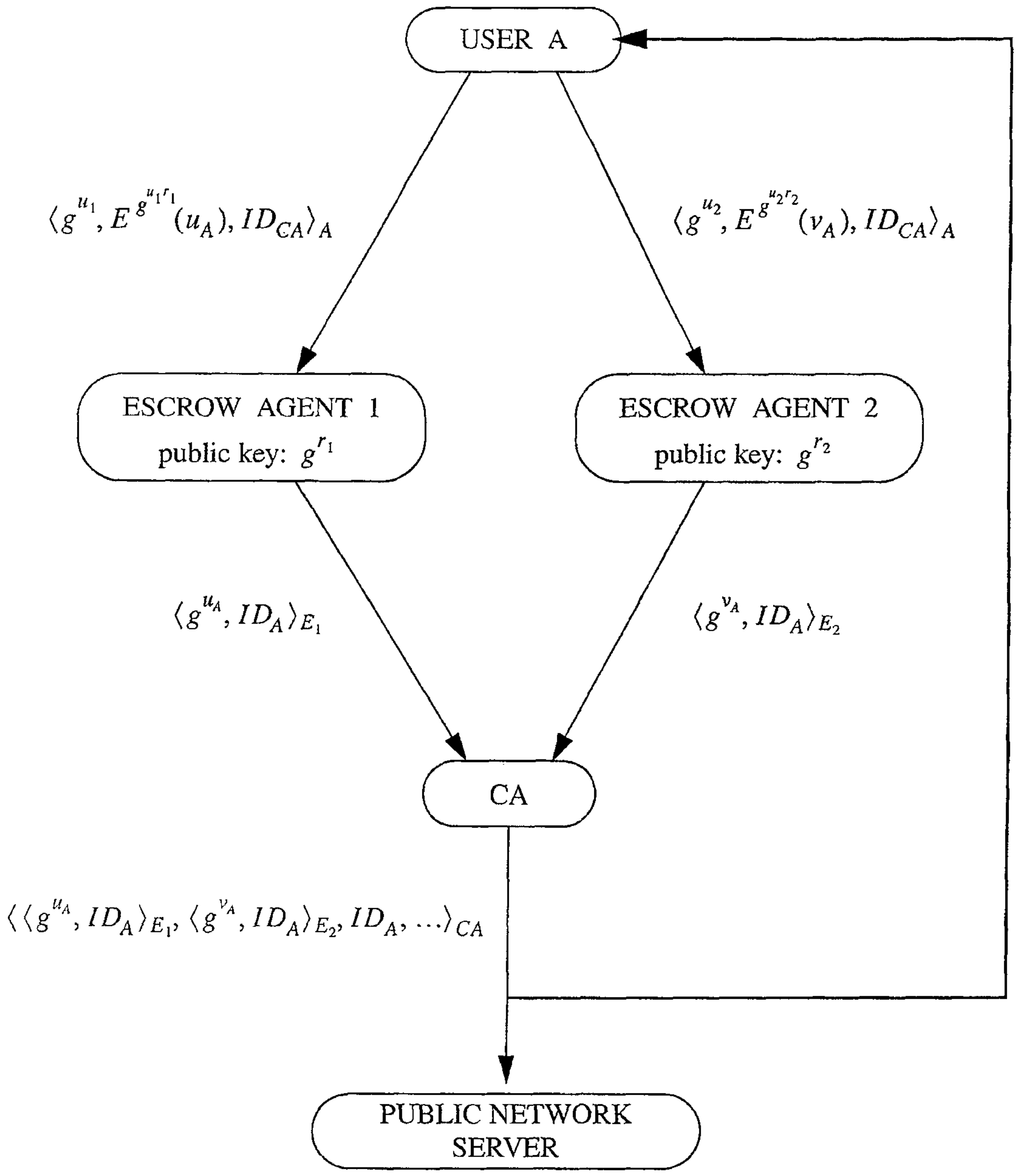
[redacted]

FBI

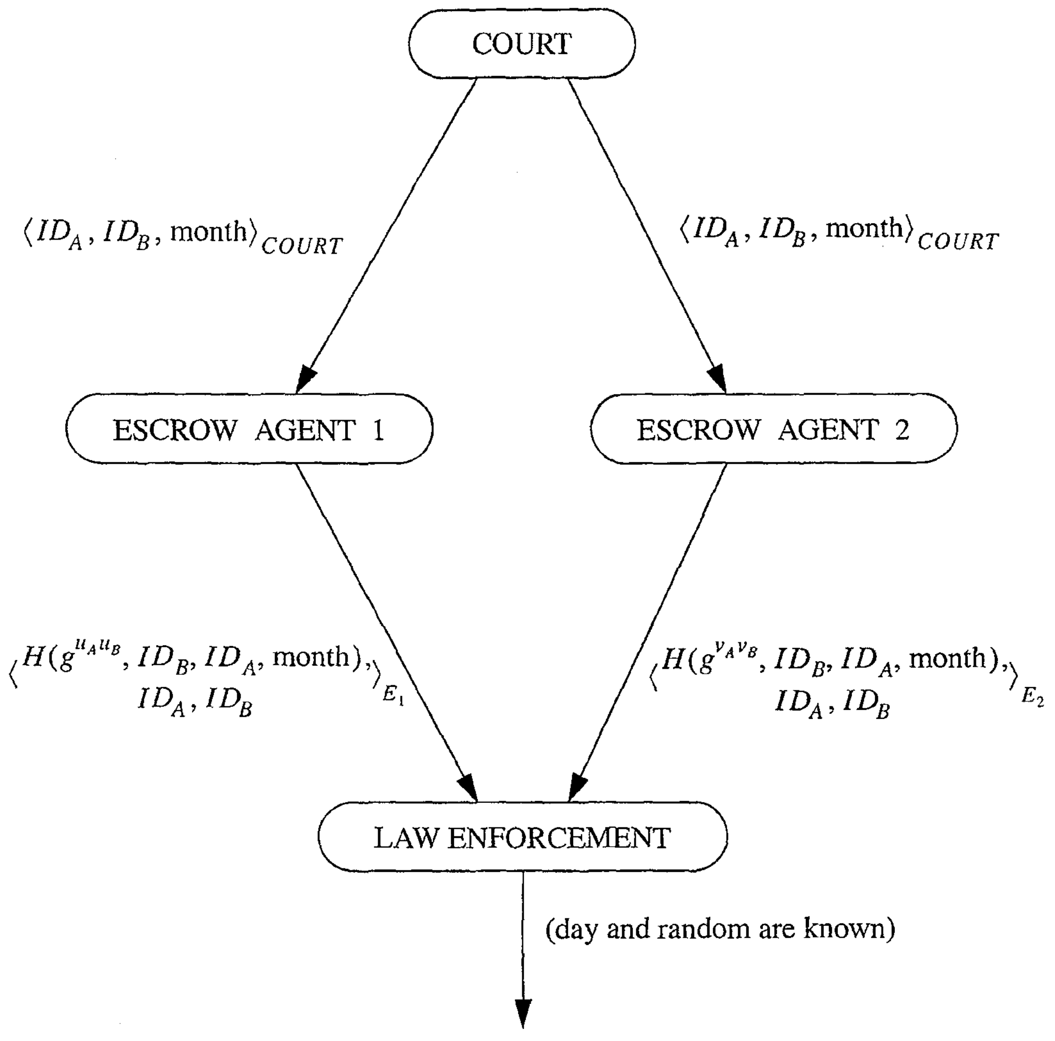
4. Data Recovery

Users may contract with a Data Recovery Center (DRC) to provide data recovery services for their data at rest. The DRC will be a valid user in the PKI, complete with a public key certificate(s) and public signature certificate(s). To save an encrypted file, the user will encrypt it with the session key derived from the DRC's public key. In other words, the session key will be derived *as if* the data was being encrypted *for* the DRC--only it will not be sent to the DRC. If data recovery is needed, the user will forward the file header information to his DRC. The DRC, in turn, will compute from the header the common session key and return this value to the user. With the session key, the user can now read his file.

NOTES: Data recovery is distinct from key escrow - a unique feature of this PKI. Also, the DRC does not need to decrypt any messages for the user, it merely gives the user the session key used to encrypt the file. The user, then, decrypts his own file--another unique feature. However, given access to the cipher, the DRC can decrypt the file.


USER A
$\langle g^{u_1}, E^{g^{u_1 r_1}}(u_A), ID_{CA}\rangle_A$
$\langle g^{u_2}, E^{g^{u_2 r_2}}(v_A), ID_{CA}\rangle_A$
ESCROW AGENT 1
public key: g^{r_1}
ESCROW AGENT 2
public key: g^{r_2}
$\langle g^{u_A}, ID_A\rangle_{E_1}$
$\langle g^{v_A}, ID_A\rangle_{E_2}$
CA
$\langle\langle g^{u_A}, ID_A\rangle_{E_1}, \langle g^{v_A}, ID_A\rangle_{E_2}, ID_A, \ldots\rangle_{CA}$
PUBLIC NETWORK SERVER

Key Escrow Mechanism


COURT
$\langle ID_A, ID_B, \text{month} \rangle_{COURT}$
$\langle ID_A, ID_B, \text{month} \rangle_{COURT}$
ESCROW AGENT 1
ESCROW AGENT 2
$\left\langle \begin{matrix} H(g^{u_A u_B}, ID_B, ID_A, \text{month}), \\ ID_A, ID_B \end{matrix} \right\rangle_{E_1}$
$\left\langle \begin{matrix} H(g^{v_A v_B}, ID_B, ID_A, \text{month}), \\ ID_A, ID_B \end{matrix} \right\rangle_{E_2}$
LAW ENFORCEMENT
(day and random are known)

$$SK = \begin{matrix} H(\, H(H(g^{u_A u_B}, ID_B, ID_A, \text{month}), \text{day}) \oplus \\ H(H(g^{v_A v_B}, ID_B, ID_A, \text{month}), \text{day}), \text{random}\,) \end{matrix}$$

Law Enforcement Access