





# **Design Criteria**

- Key-escrow capability
- All system components are public
- All default algorithms are well-known
- User has choice of encryption algorithm
- Data recovery distinct from escrow mechanism
- Encryption session key computed via one sided exchange (recipient does not have to *actively* participate)
- Scalable to large number of users
- Interoperable with other systems

# **Privacy Features**

- Only the user knows her private signature key
- Disclosure of user encryption secrets requires collusion of escrow authorities
- CA and DRC holds no user secrets
- Warrant service does not compromise any user secrets
- Warrants can be bounded both in time and direction
- Users have option to generate their own secrets

#### DCID: 3219128

## **Customer Features**

- Modular, flexible design
- Low infrastructure overhead per message (no LEAF)
- Escrow registration requires low software overhead
- Default protocols are specified, guaranteeing a secure communications path
- Participants can verify that correspondents are also participants

# Ingredients

## **AUTHENTICATION**

- Private and public signature key pair
- Proof of identity

## **ENCRYPTION**

- Universal base g and prime p
- Escrowed, secret encryption keys  $u_A$  and  $v_A$
- Public encryption keys  $g^{u_A}$  and  $g^{v_A}$
- A secure hash algorithm *H*







# **Encrypted Message from B to A**

• Session Key:

SK = SK(B, A, month, day, random)

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

• month, day, and random sent in clear:

header, month, day, random,  $E^{SK}(\langle m \rangle_{R})$ 

header, month, day, random,  $E^{SK}(CV), E^{CV}(\langle m \rangle_B)$ 





# **Roles and Requirements**

The Policy Authority (PA) will:

- Establish and develop standards
- Determine default algorithms
- Certify PKI compliance
- Authenticate CAs and EAs
- Issue and respond to security alerts
- Foster international agreements

# **Roles and Requirements**

An Escrow Authority (EA) will:

- Escrow, archive and protect users' split keys
- Process warrants
- Register public encryption keys
- Create secret encryption keys for a user upon request
- Provide secret key recovery for users

# **Roles and Requirements**

A Certificate Authority (CA) will:

- Bind users' identities to public signature keys
- Sign public key certificates and post them to network
- Archive users' signature certificates for a time specified by law
- Issue revocation certificates to the public network