National Immunization Program Aspects on Security Confidentiality and Privacy

Gunther Schadow
Clem McDonald

Regenstrief Institute for Health Care

Atlanta, GA, Junly 31, 1998

Assets and Risks

- **What information will be stored?**
  - Immunization record (not the whole medical record, not even its core)
  - Patient index data (name, DOB, genealogy, SSN, UHI, etc.)
  - Patient demographics (address, phone number)
- **What is at risk?**
  - The immunization record is probably the least interesting information although it may sometimes allow infering an impaired health condition or a likely diagnose.
  - The index may be a directory to unlock other sources of data, or for simple SSN fraud.
  - Patient demographics is of tremendous value, attempts will be made to exploit this commercially, criminally and for law enforcement.

➡ **The credibility of the NIP is at risk.**

➡ **Separating out the core data may not help much.**

Confidentiality of Information

- A Policy has to be in place to regulate who may access what information about whom (rules).
- Access rights have to be determined for each transaction request (decision).
- Information in transit must be encrypted to deny general read access to eavesdroppers.
- System integrity and operation must be maintained and information loss prevented.

Policy

- **Define roles:** both human and process roles.
  - Human Roles: Patient, Doctor, System administrator.
  - Process Roles: Provider IS, Registry, Index, Birth registry.
- **Define data:** use modeling tools to visualize.
  - Provider, Patient, Immunization, Vaccine, Reaction.
- **Define transactions:**
  - What objects are involved?
  - What objects are affected?
- **Define which transactions may be initiated by which roles.**

Authorization

- **Who is the initator?**

  Identification: design the namespace in which identifiers are meaningful.

  Authentication: apply technology to assure the integrity of identification information.

- **What are the rights of that initiator?**

  Authorization:

  1. **Role based (absolute rights)**

     Every doctor may retrieve every imunization record.

  2. **Subject based (relative rights)**

     The doctor of patient X may retrieve the record of patient X.

Authentication

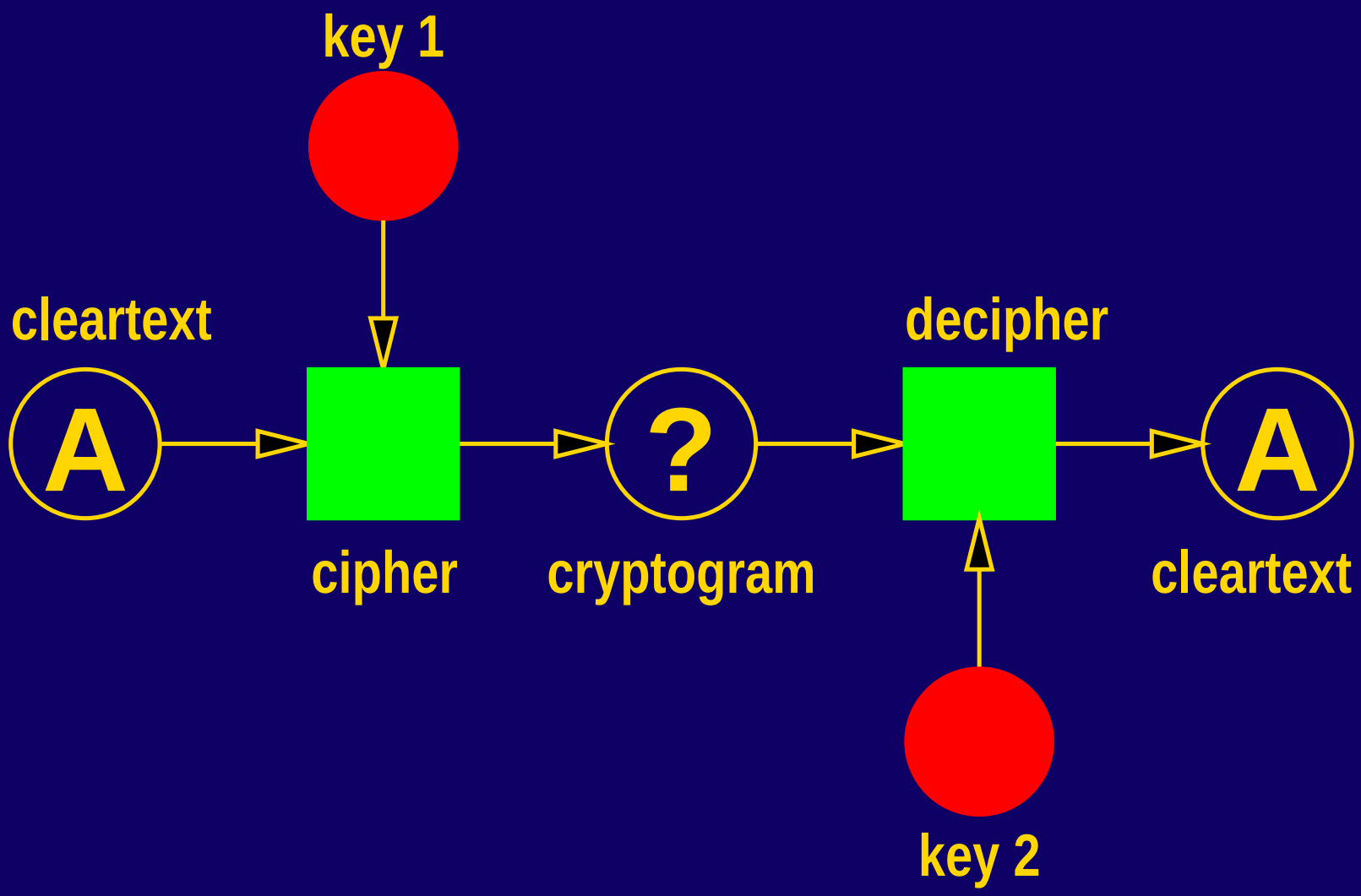
- **Passwords:** most commonly used, easily implemented
  Passwords can be guessed, stolen, and intercepted

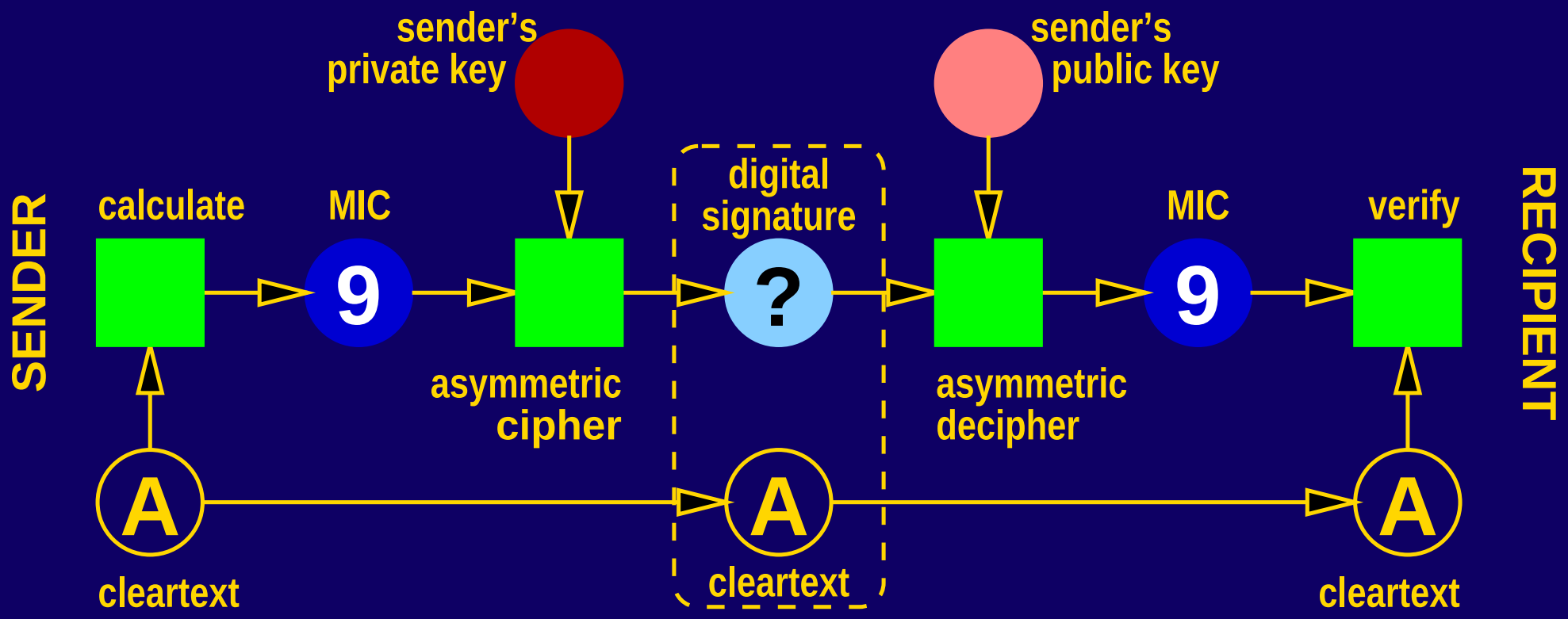
PASSWORDS ARE BAD

- **One-time passwords:** e.g. Kerberos, S/Key
  + Guessing is very hard, intercepting makes little sense
  - Require the user to keep a device or a list of passwords, subject to theft, or again interceptable initial passwords.

- **Digital signature:** similar to challenge-response method.

- **Certificate exchange:** e.g. used by SSL and secure MIME.


key 1
cleartext
A
cipher
?
cryptogram
decipher
A
cleartext
key 2

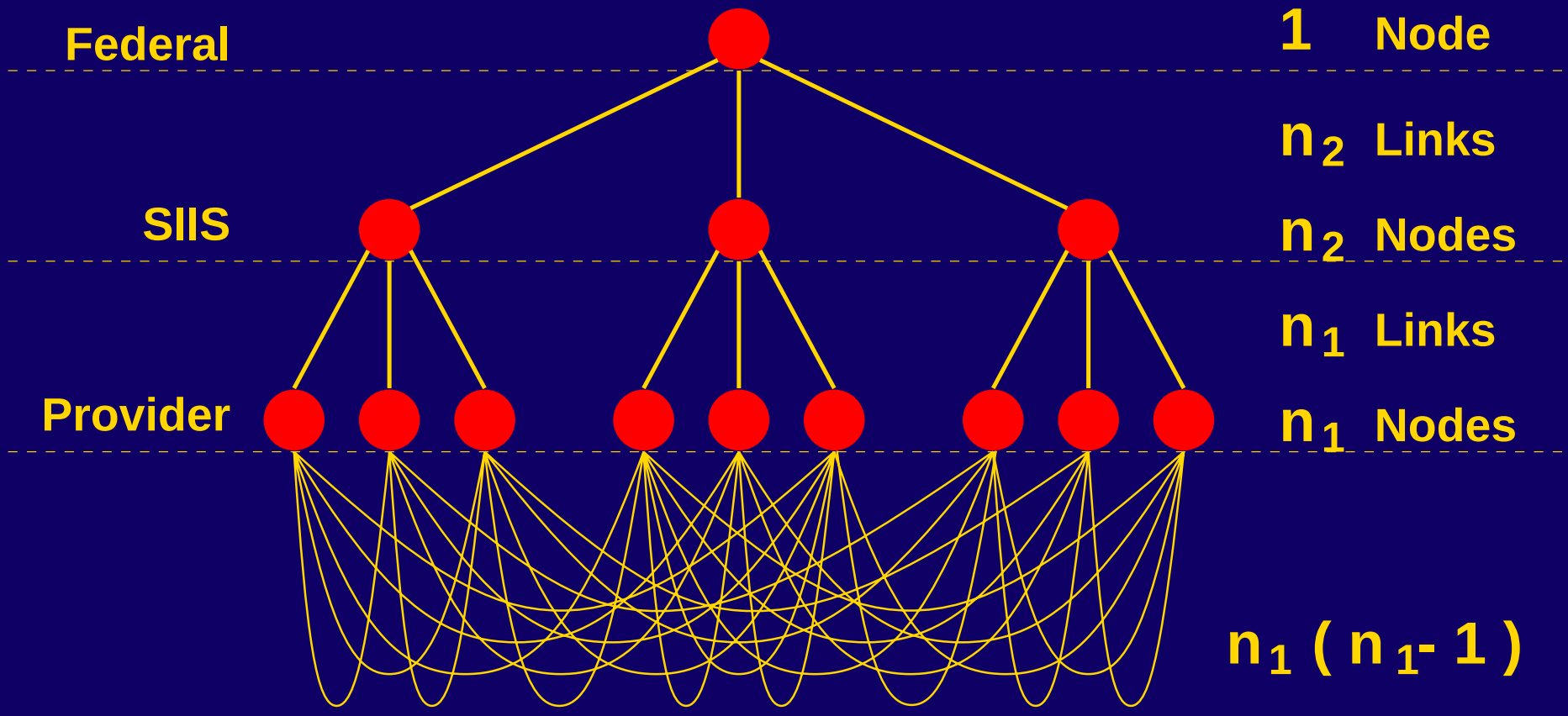

sender's
private key
sender's
public key
digital
signature
SENDER
calculate
MIC
MIC
verify
RECIPIENT
9
?
9
asymmetric
cipher
asymmetric
decipher
A
A
A
cleartext
cleartext
cleartext

- A certificate is a name and a public key signed by someone else.
- Senders and receivers have to trust the one who issued the certificate.
- Certificate issuing is crucial to security ...

  It is paramount to trust the certificate issuer!
- ... certificate distribution is not security relevant.

  You can accept certificates from everywhere as long as you trust the signature on it.

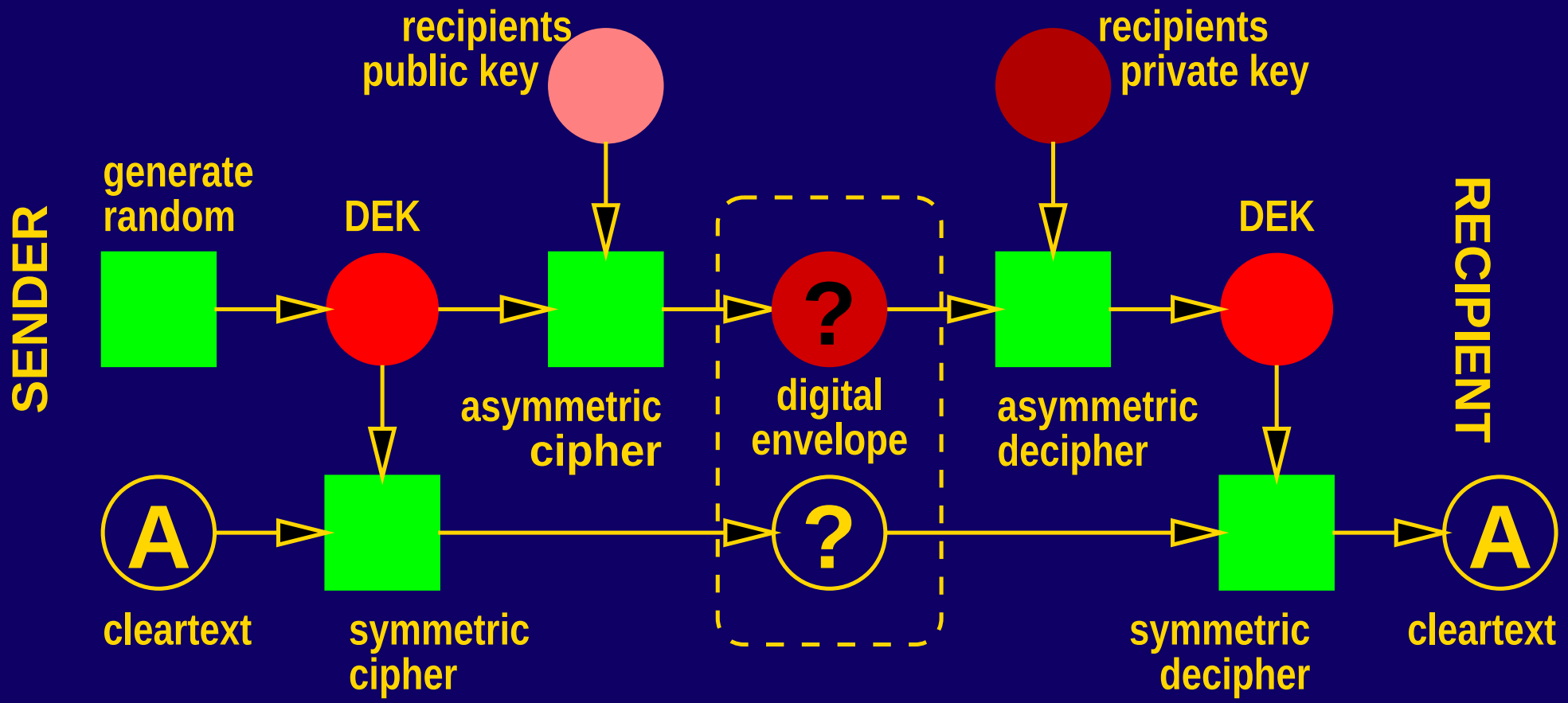
- Impact of the virtual network topology:



➡ Hierarchical organization reduces complexity!

Encryption

- All patient data in transit must be encrypted.
- The digital Envelope:



Site Security

- Firewalls should protect all immunization record and index systems connected to public networks.
  - Also holds for servers on telephone lines (dialup servers).
  - Firewalls are separate machines that provide no other services.
  - Packet filters are not enough, application layer gateways prefered.
  - Only sites that can run a firewall properly should act as servers.
- Encryption of data on site is not required if physical protection is made sure.
- Only strong SmartCard based authentication to log in on sites. No passwords!
- Rigorous backup scheme, disaster plans.

Privacy

- We should regard the patient (or his legal guardian) as the owner of his record.
- The patient, not the doctor, has to decide whether his immunization record is kept, updated, or communicated.
- The patient has a right to see his complete record.
  - But how do we authenticate patients?
- Maintain a clear scope how patient data is used.
  - Do not break a promise: do not permit use for other purposes.
- Keep the public informed, establish public control mechanisms.

Open Issue

How can we make sure that only a doctor who actually takes care of a given patient can retrieve this patient's record?

- **There is no strong association between patients and physicians.**
- **Patients could carry an authenticator token - but why not let them carry the record in the first place?**