Goal:

Create a component to exchange IODEFs between real incident handling systems

---

Goals defined in the project

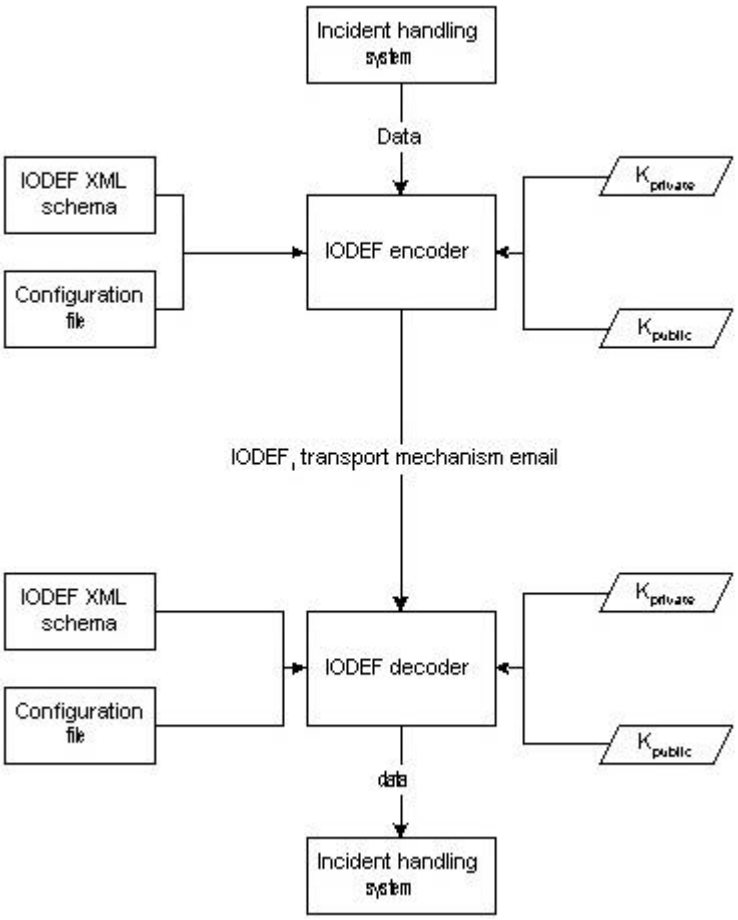
- To implement IODEF in practice of CSIRTs participating in the project, CERT-NL and JANET-CERT
- To develop special API modules for plugging IODEF based Incident descriptions to and from incident handling/tracking used by CSIRTs
- To develop XML parser based on XML DTD (or Schema) to convert data to/between database formats used by CSIRTs
- Produce guidance for API development by other teams for their own specific incident handling tools
- To progress with Internet Drafts and further development of Extended Incident Handling Scheme based on experience acquired
- Promote use of IODEF by showing it actually works :)

Effort, timetable

- CERT-NL (SURFnet) and JANET each contribute 25 mandays
- Terena puts in 1/8 FTE
- Work will take place from September 2001 until August 2002

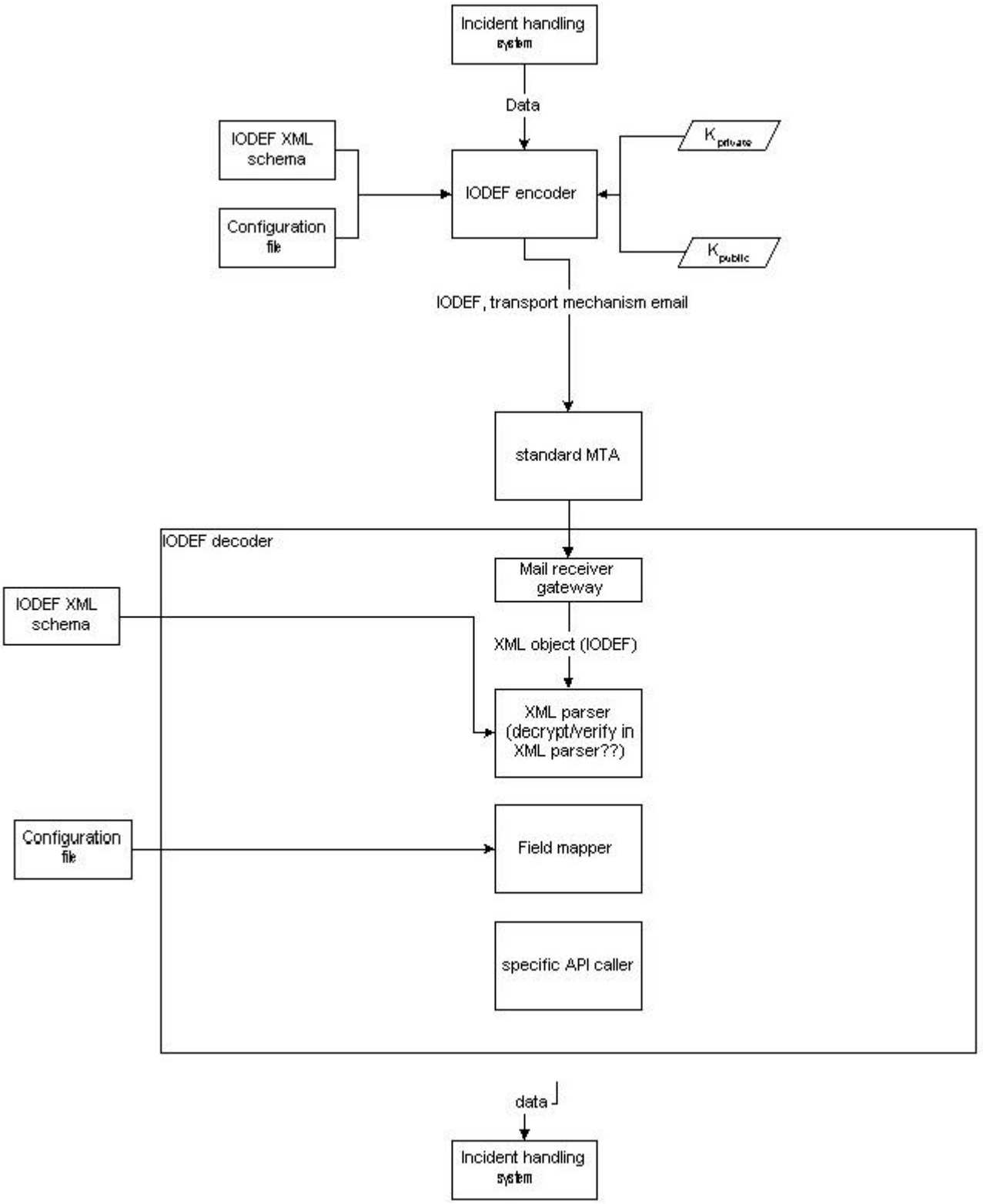
Design ideas

- A gateway to exchange IODEFs between differently built incident handling systems, not an incident handling system
- Ability to sign the XML objects and to verify the signature is very important
- Use configurable mapping between IODEF data and system specific data
- Use mail for exchange of IODEFs (robust, available everywhere



Diagram

Bit more detailed ideas (work in progress):


Incident handling system
Data
IODEF XML schema
Configuration file
IODEF encoder
$K_{private}$
K_{public}
IODEF, transport mechanism email
standard MTA
IODEF decoder
Mail receiver gateway
IODEF XML schema
XML object (IODEF)
XML parser (decrypt/verify in XML parser??)
Configuration file
Field mapper
specific API caller
data
Incident handling system

Diagram