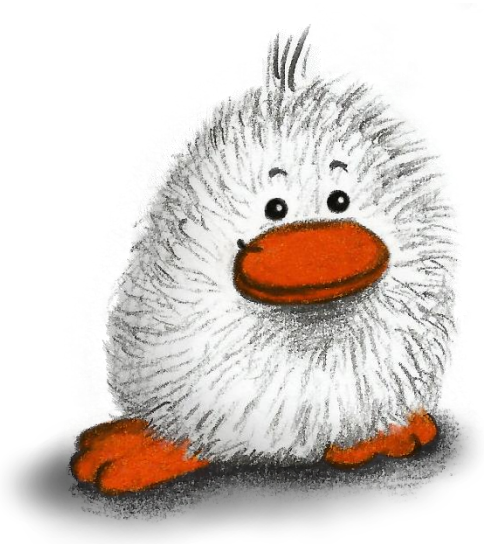
How to Break XML Encryption – Automatically

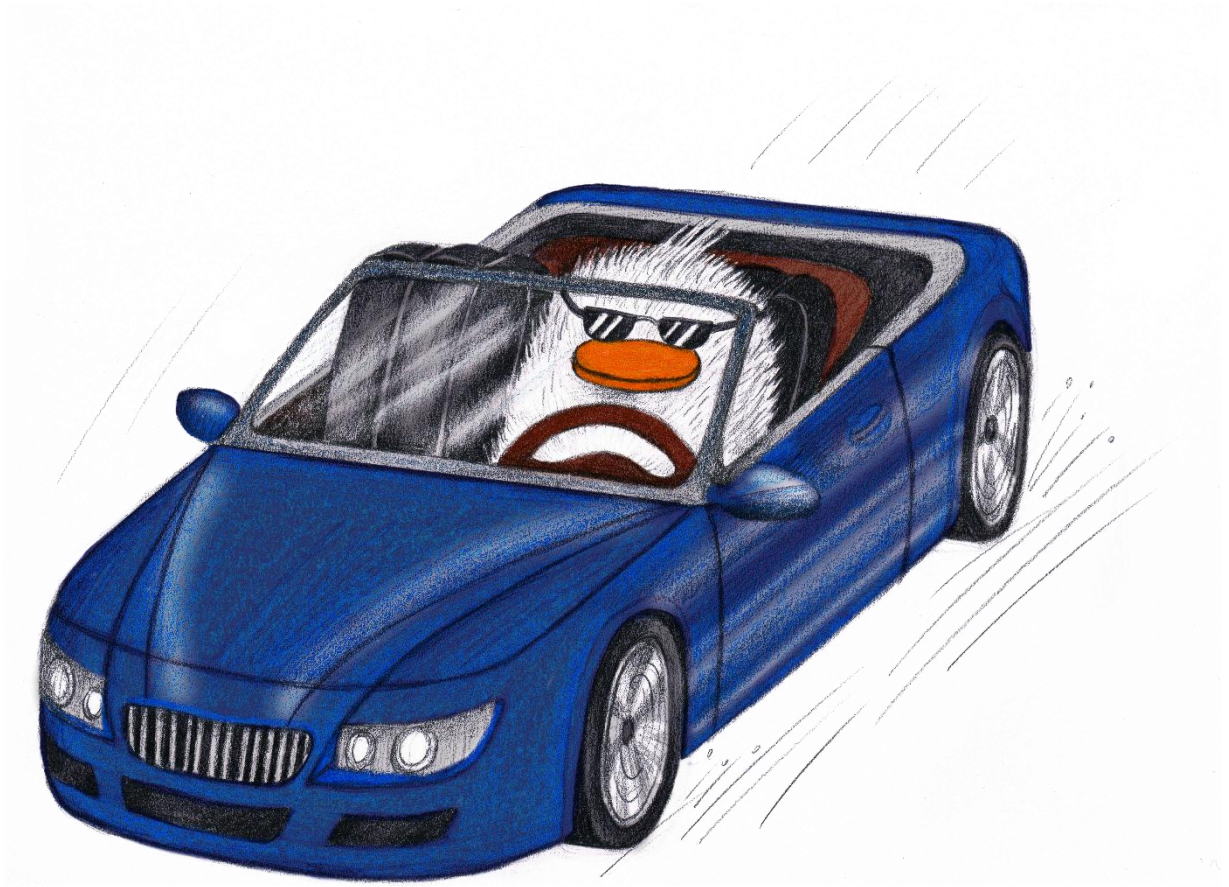
Dennis Kupser, Christian Mainka,
Jörg Schwenk, Juraj Somorovsky

Horst-Görtz Institute for IT-Security
Ruhr-University Bochum

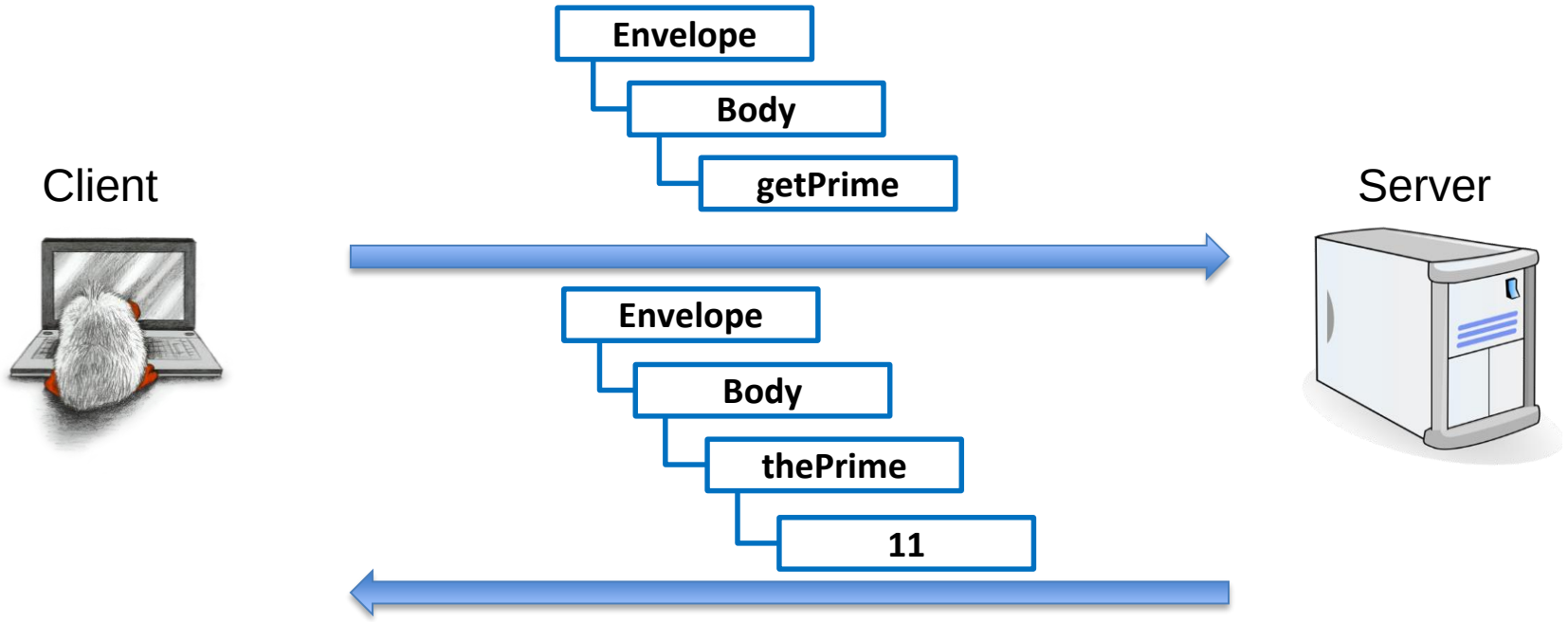
Christian.Mainka@rub.de
Twitter: @ChearíX



Quick Introduction

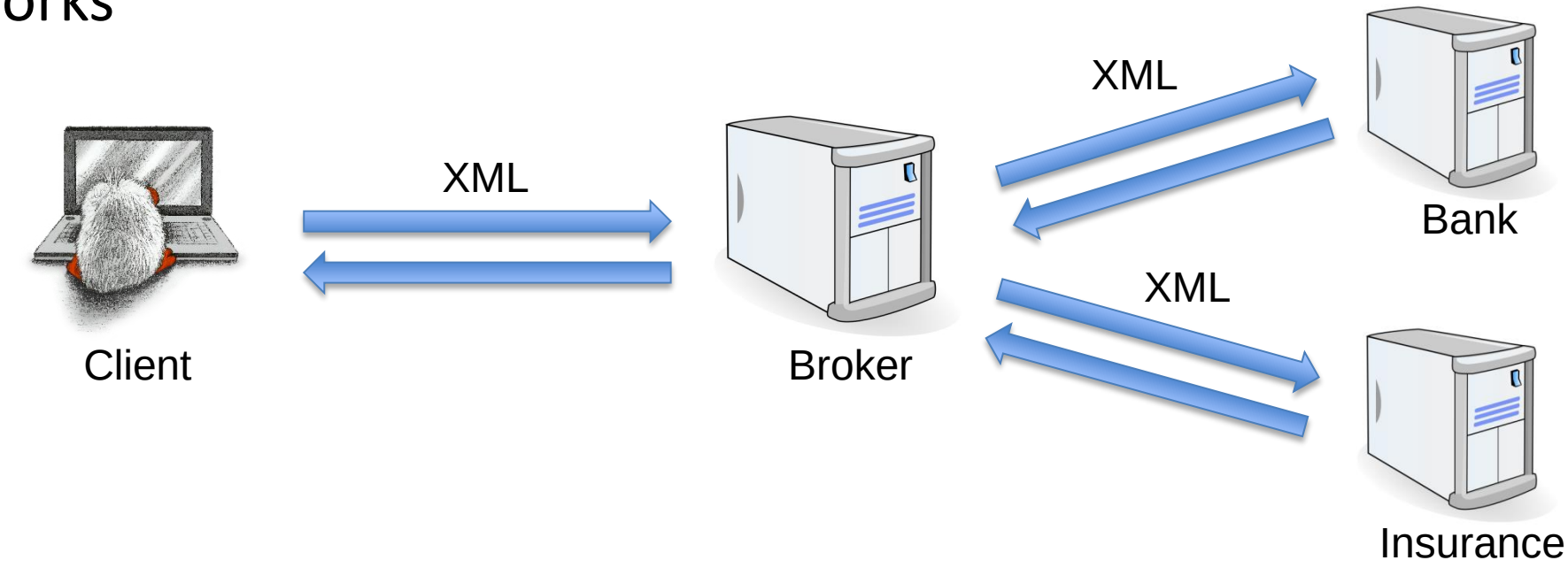


XML-based Web Service



Motivation – XML Security

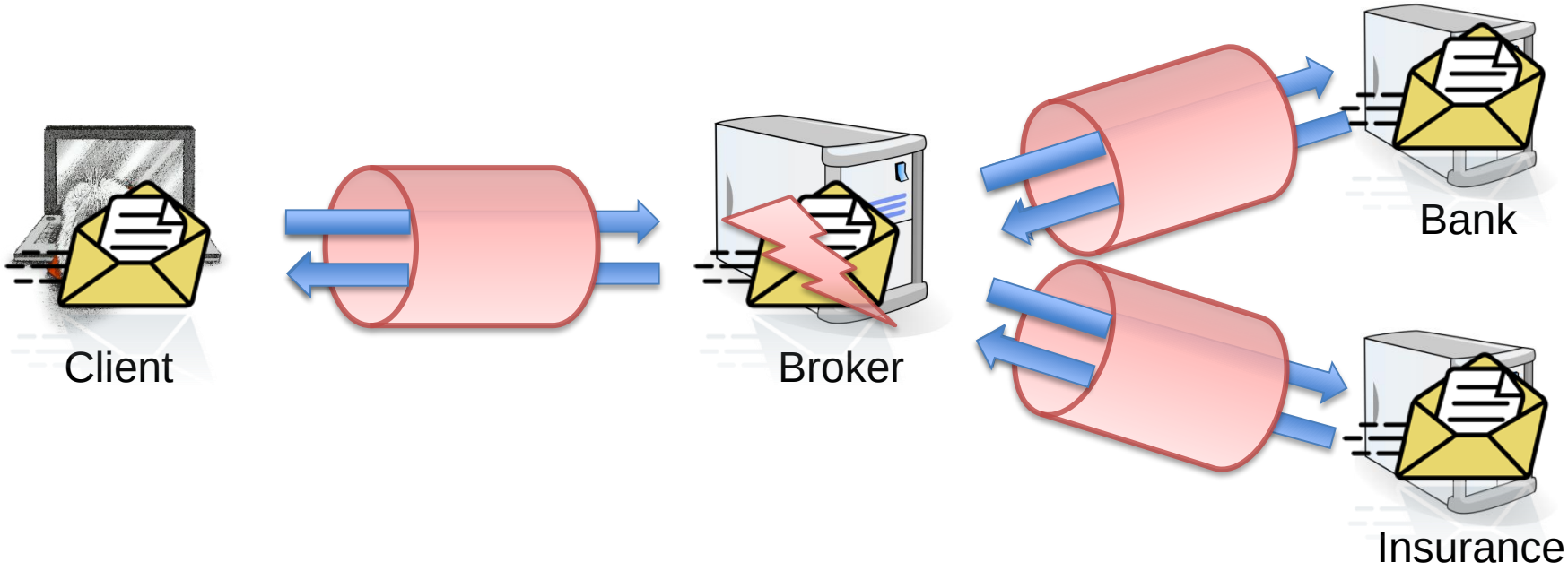
- Web Services: Method for machine-to-machine communication over networks



- Used in commerce, finance, government, military, …
- XML-based message format

Motivation – XML Security

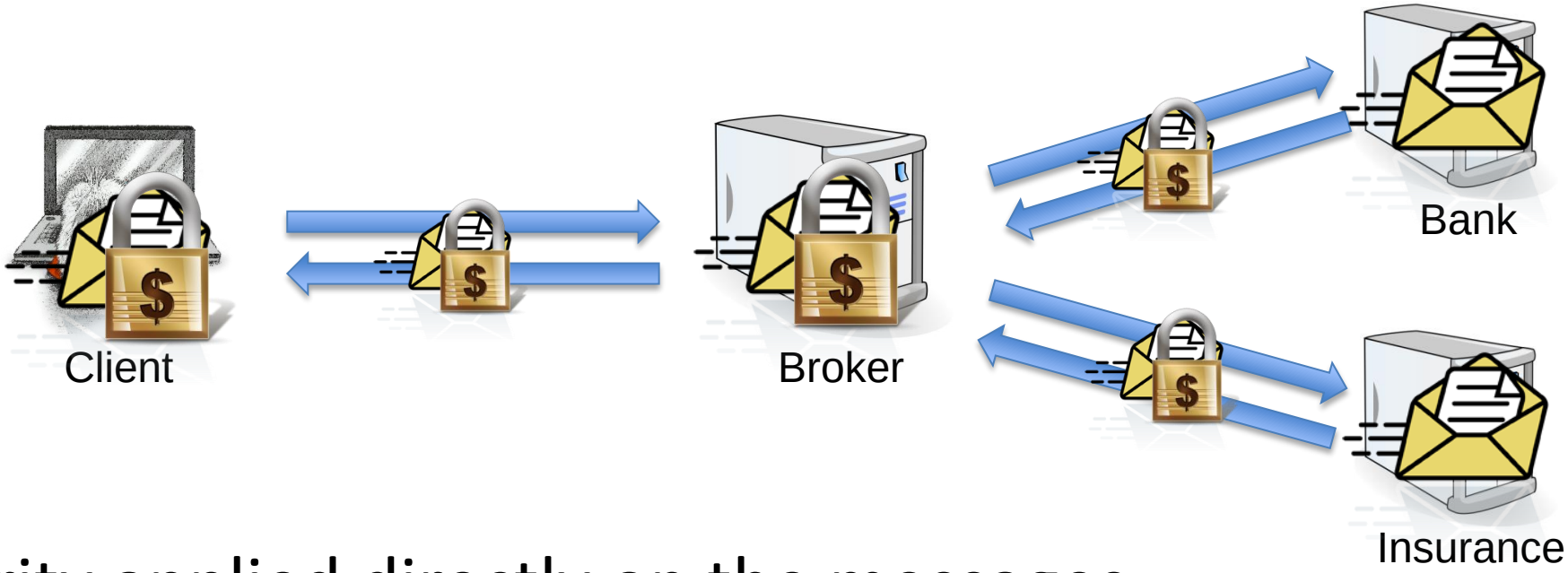
- SSL / TLS: transport-level security



- Messages secured only during transport!

Motivation – XML Security

- Message level security



- Security applied directly on the messages
- No need for SSL / TLS
- Realized using XML Signature, XML Encryption

XML Security

- W3C Standard for securing XML messages
- XML Encryption: protects confidentiality
- XML Signature: protects authenticity and integrity
- Very flexible

Dresdner Bank Die Beraterbank

Sparkasse

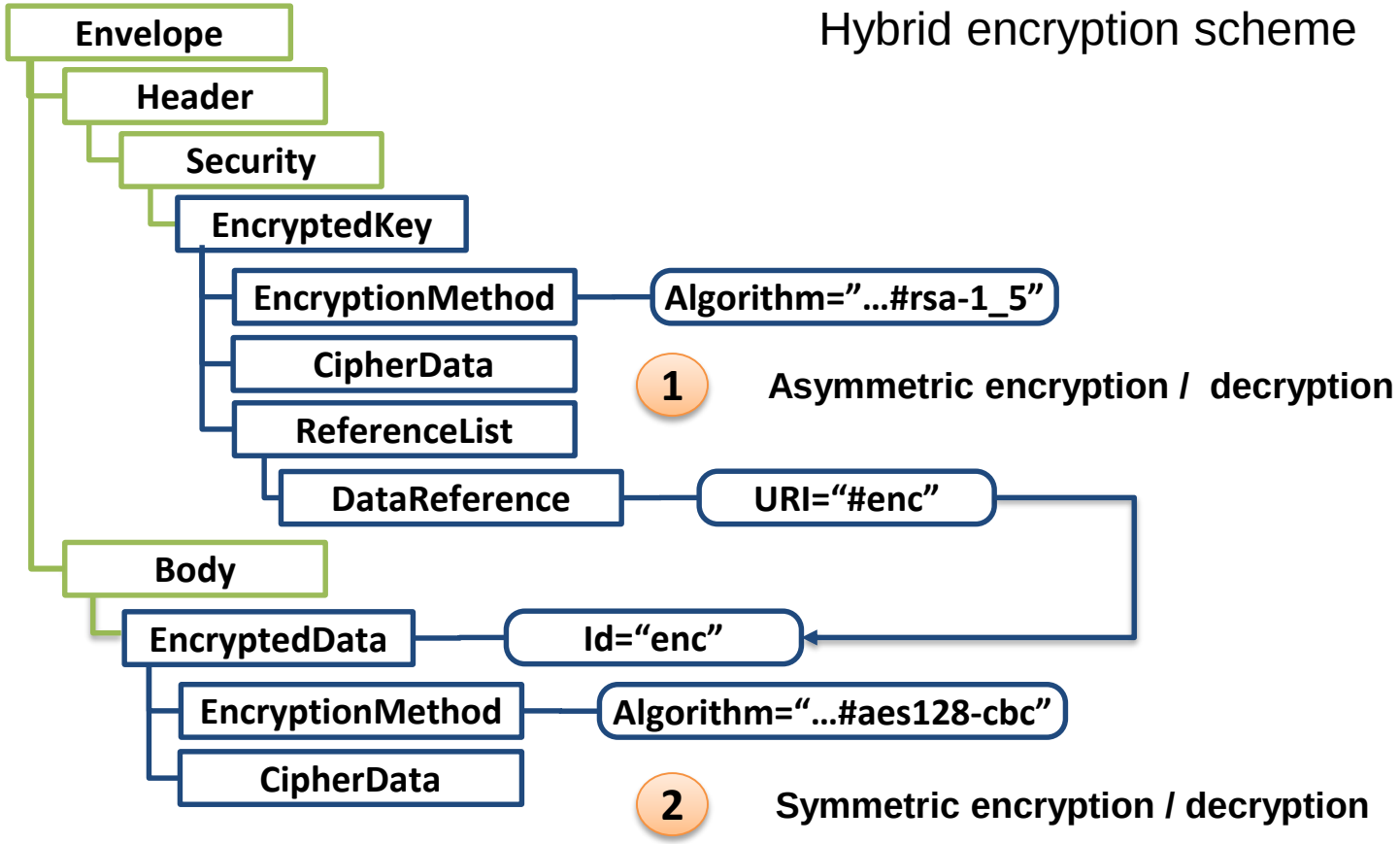
COMMERZBANK

IBM WebSphere




```
<PaymentInfo>
  <Name>John Smith</Name>
  <CreditCard Limit='5,000'>
    <Number>4019 ...5567</Number>
    <Issuer>Example Bank</Issuer>
    <Expiration>04/02</Expiration>
  </CreditCard>
</PaymentInfo>
```

XML Encryption



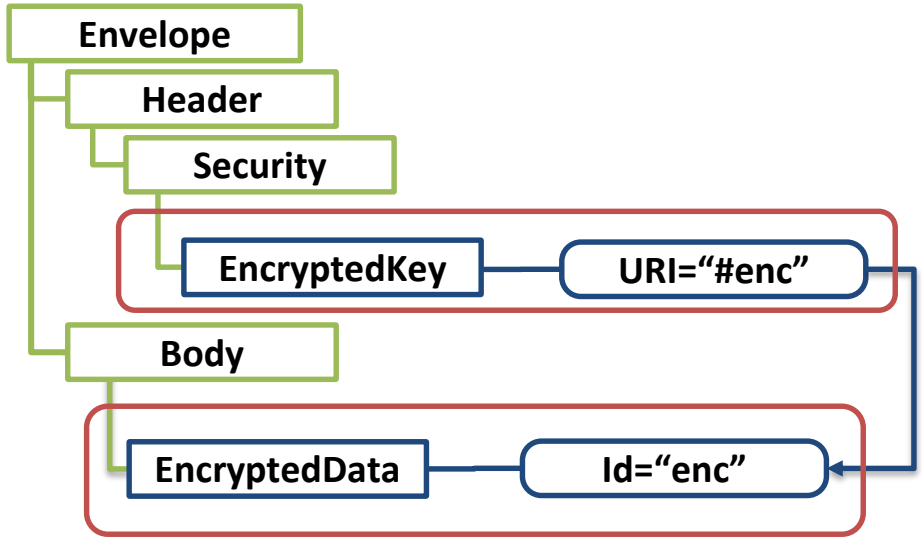
Hybrid encryption scheme

1 Asymmetric encryption / decryption

2 Symmetric encryption / decryption

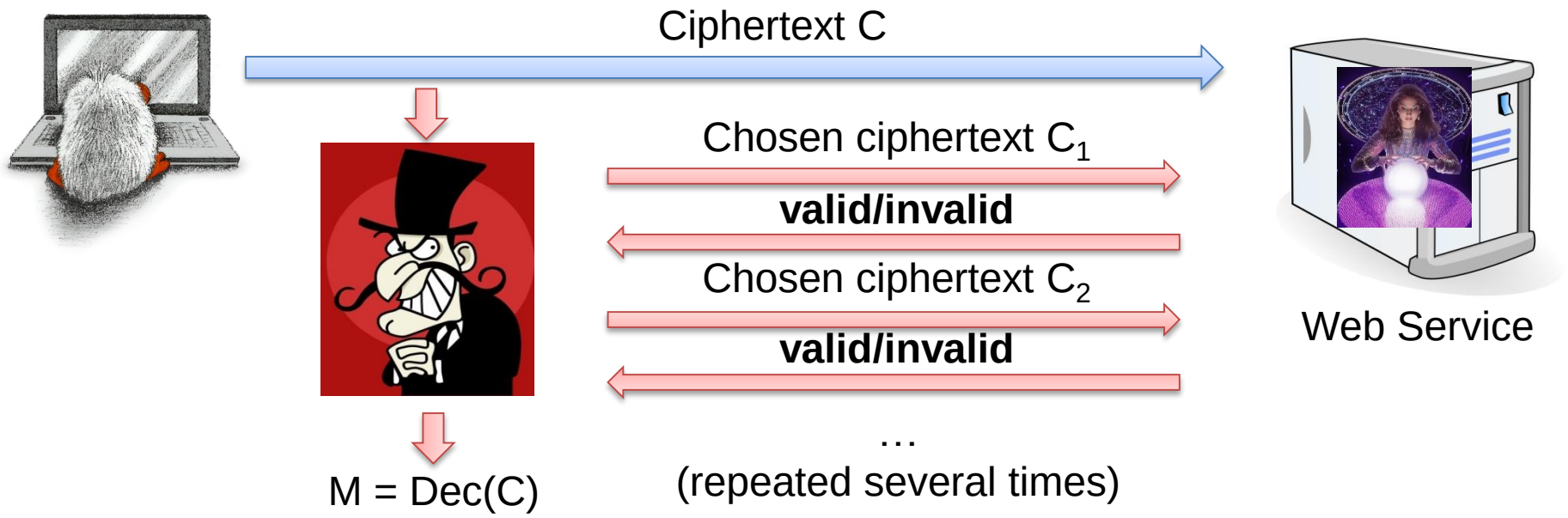
Attacks on XML Encryption

- Attacks on EncryptedData
  - How to Break XML Encryption.
    Tibor Jager, Juraj Somorovsky. CCS 2011



- Attacks on EncryptedKey
  - Bleichenbacher's Attack Strikes Again:
    Breaking PKCS#1 v1.5 in XML Encryption.
    Tibor Jager, Sebastian Schinzel, Juraj Somorovsky. ESORICS 2012

Attack Concept: *Validity Oracle*

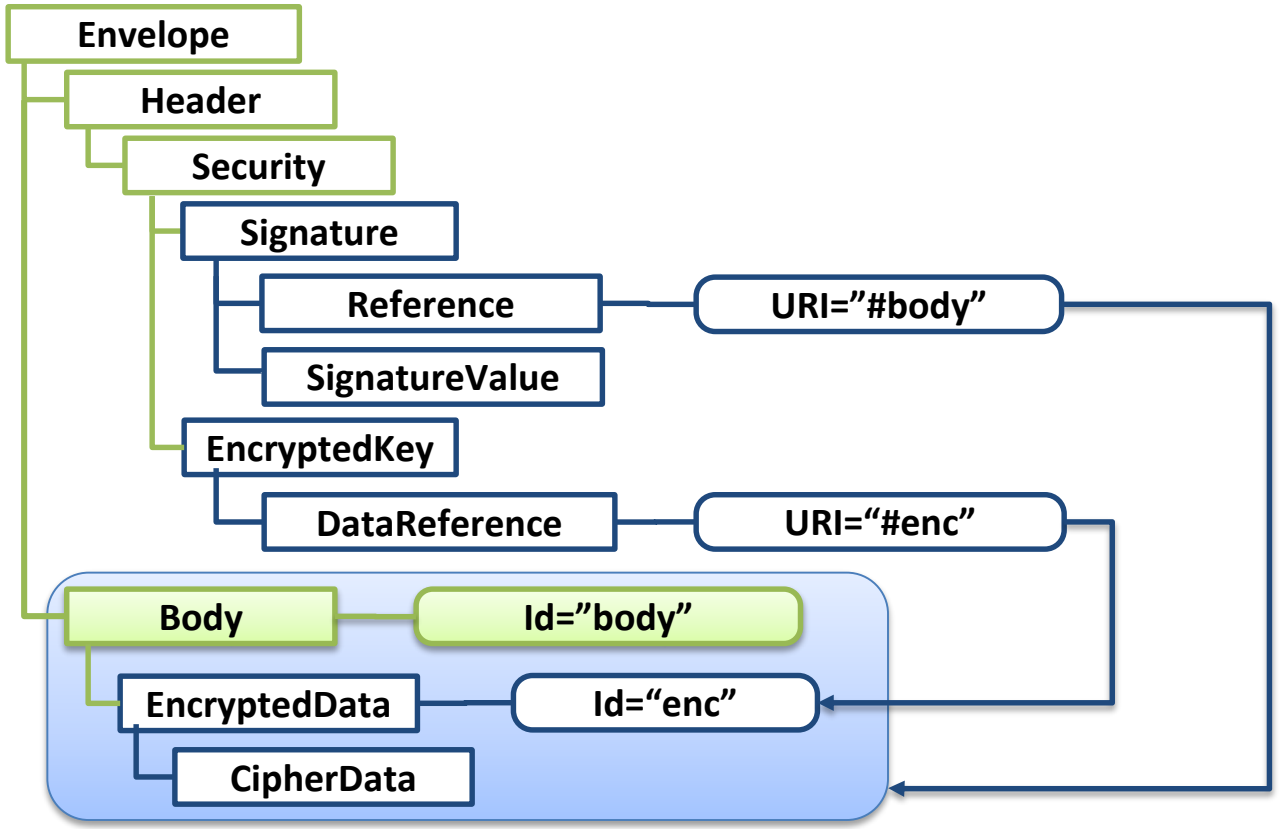


- Attacker needs to send arbitrary ciphertexts!

Countermeasures?



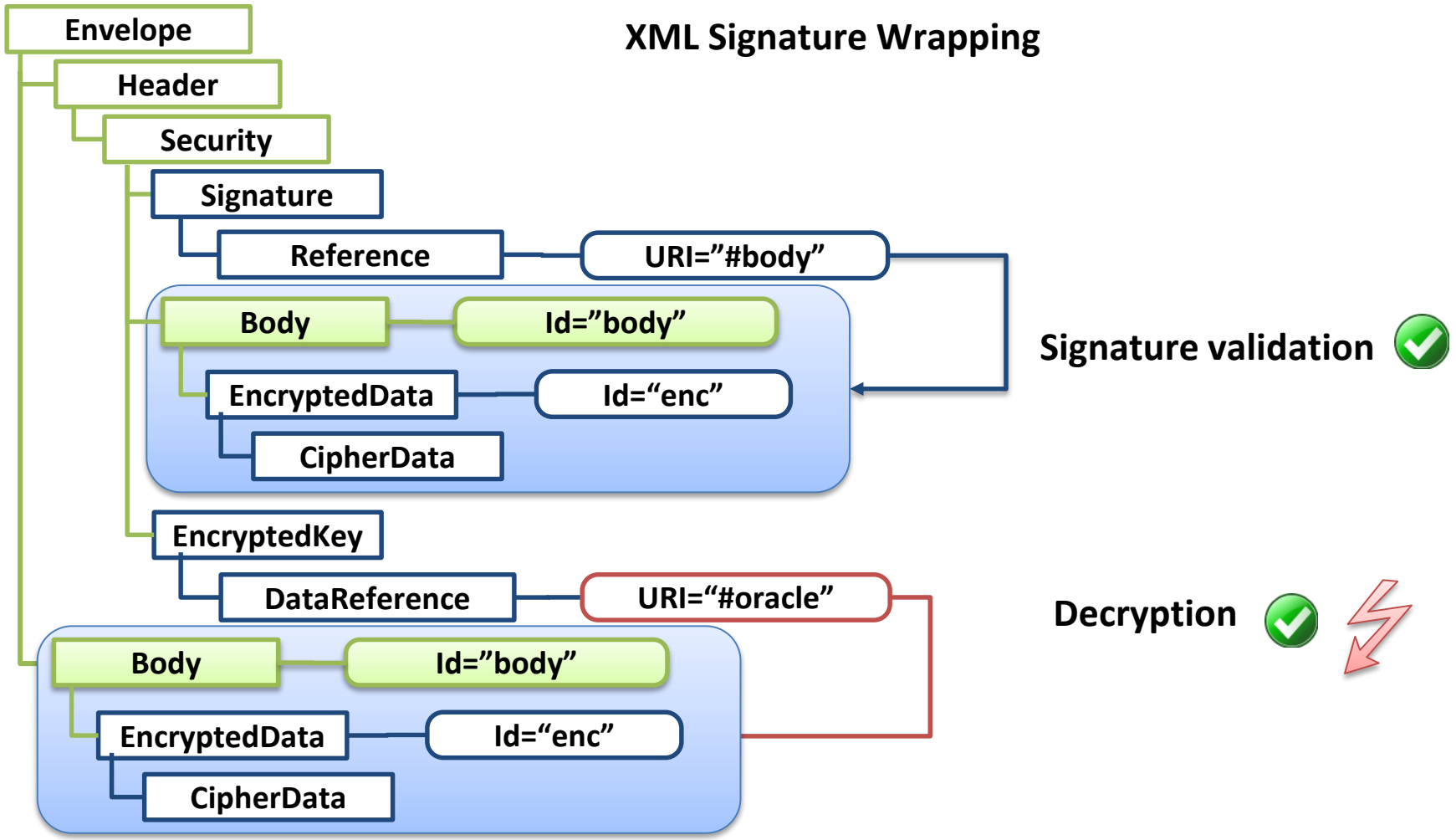
Countermeasures – XML Signature?



Attacker able to create valid signatures?

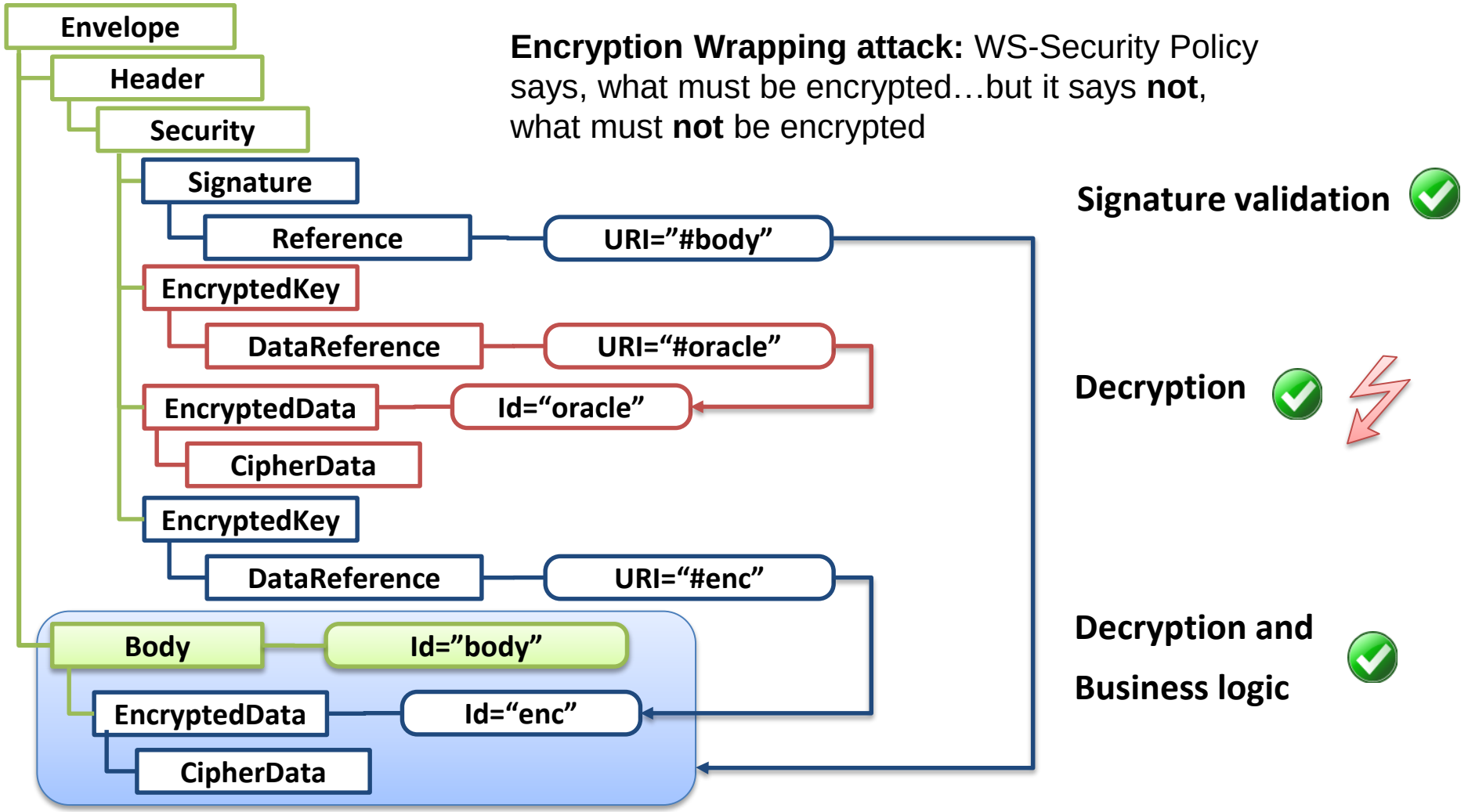


Countermeasures – XML Signature?



McIntosh and Austel. XML Signature Element Wrapping attacks, 2005

Countermeasures – XML Signature? XML Encryption Wrapping (XEW)



Encryption Wrapping attack: WS-Security Policy says, what must be encrypted…but it says **not**, what must **not** be encrypted

Signature validation

Decryption

Decryption and Business logic

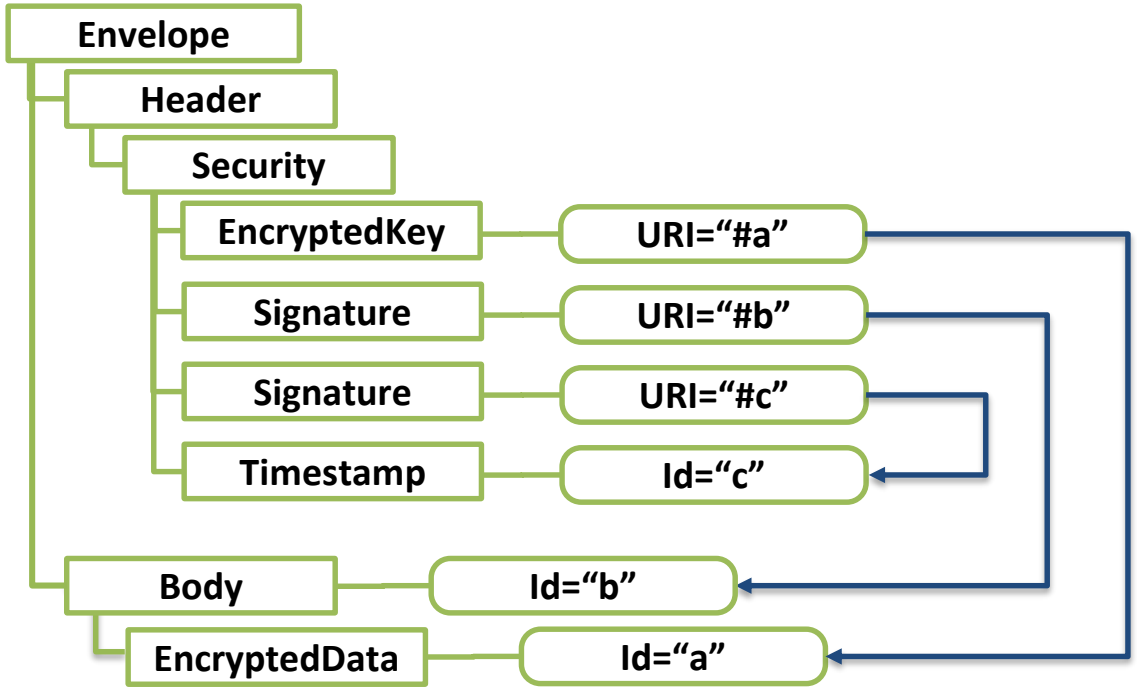
WS-Attacker Implementation



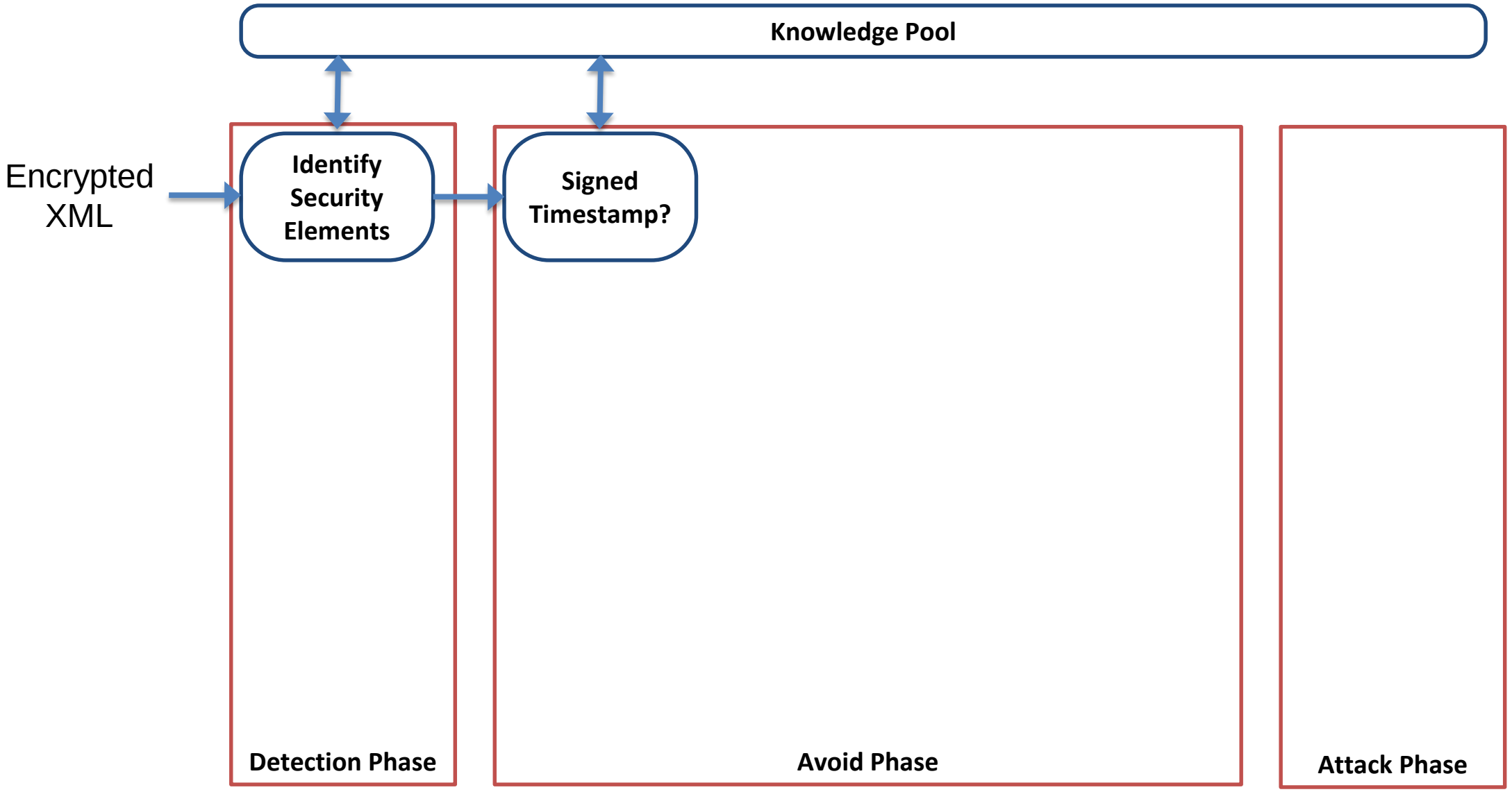
Automated Attack Workflow



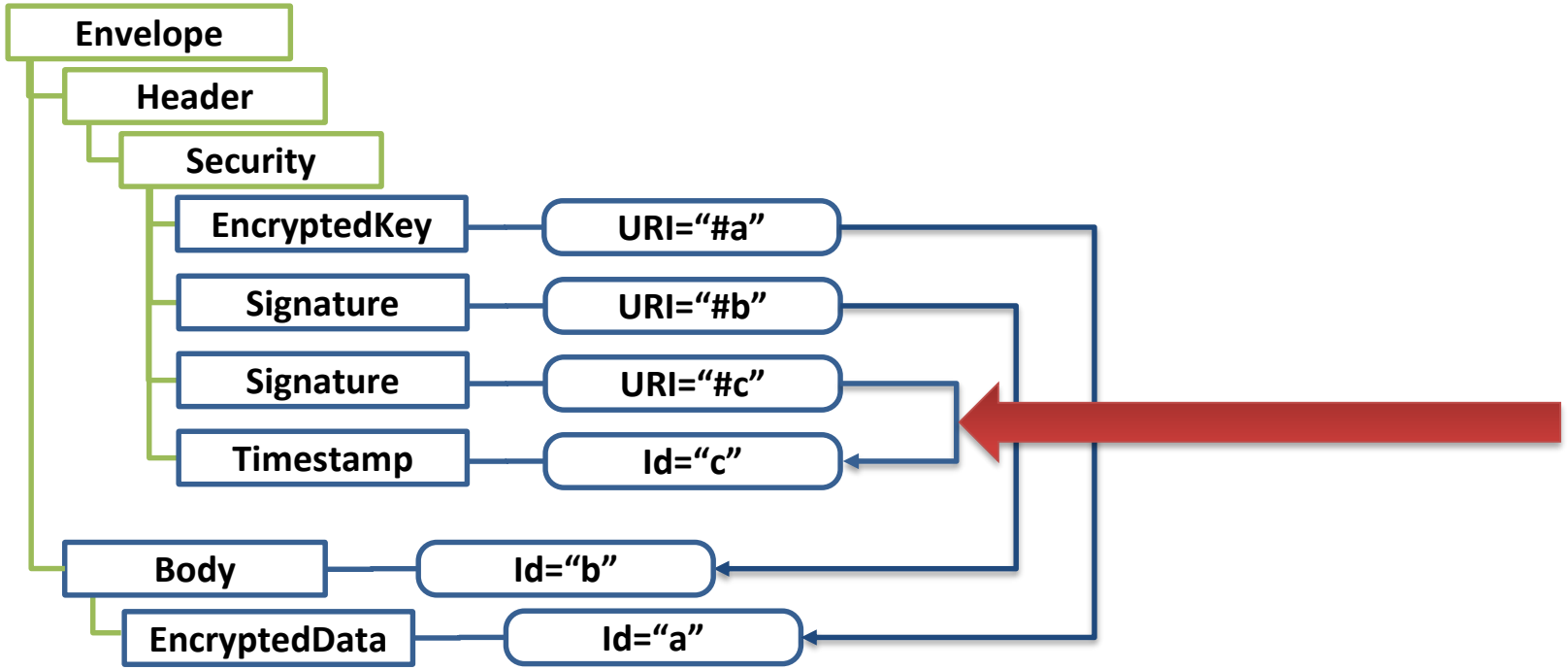
Detection Phase (Offline)



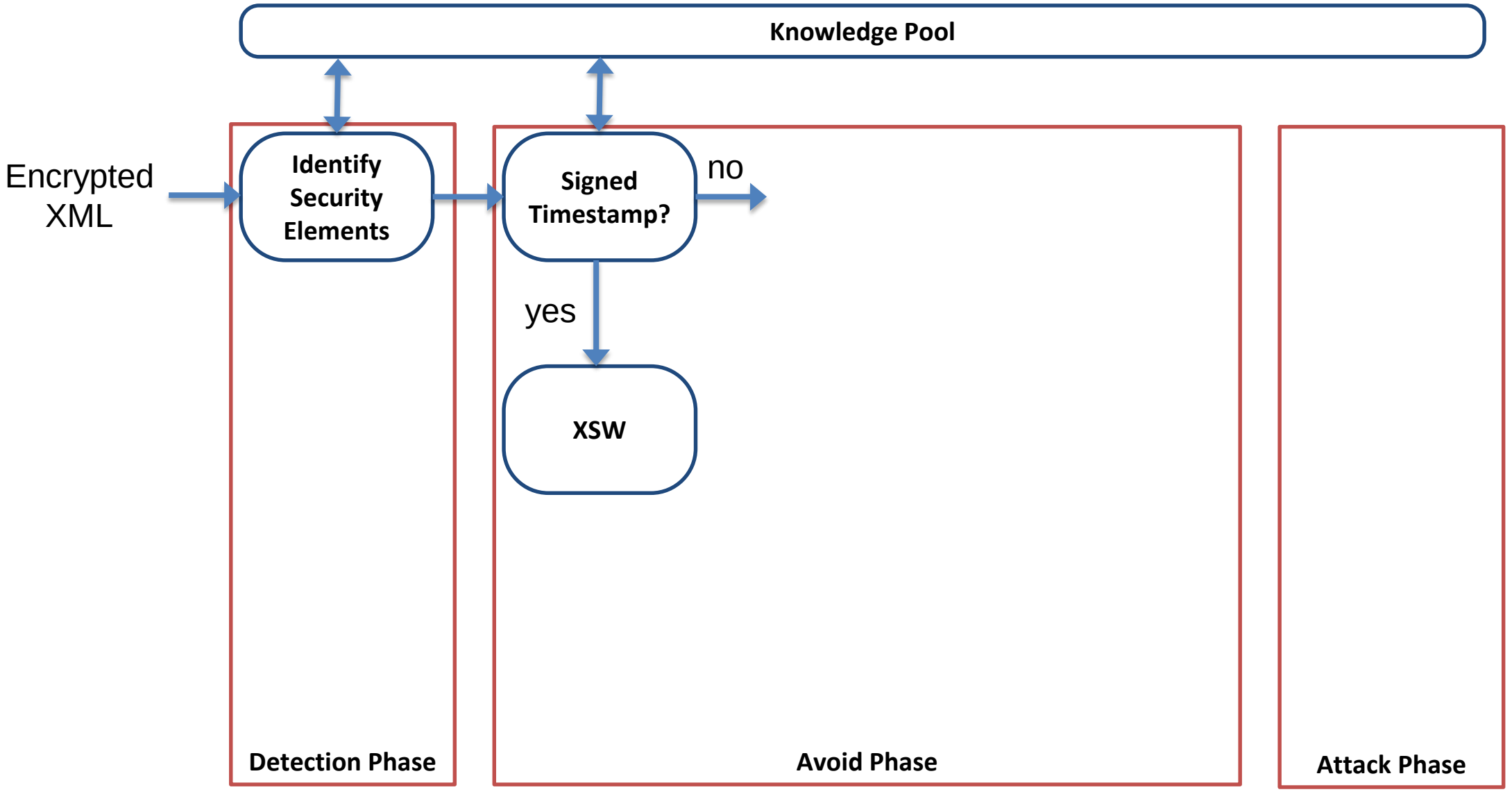
Automated Attack Workflow



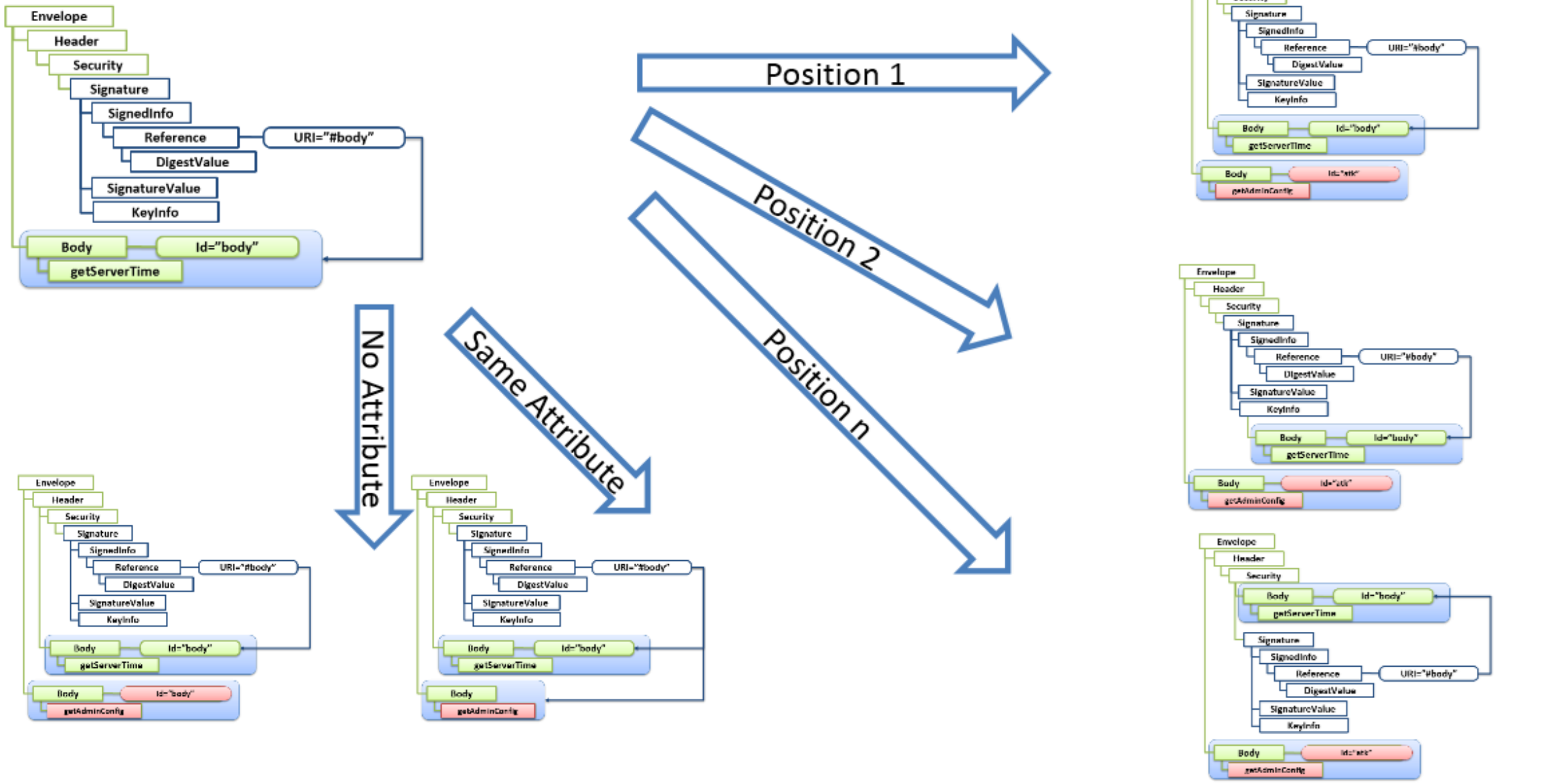
Detection Phase (Offline)



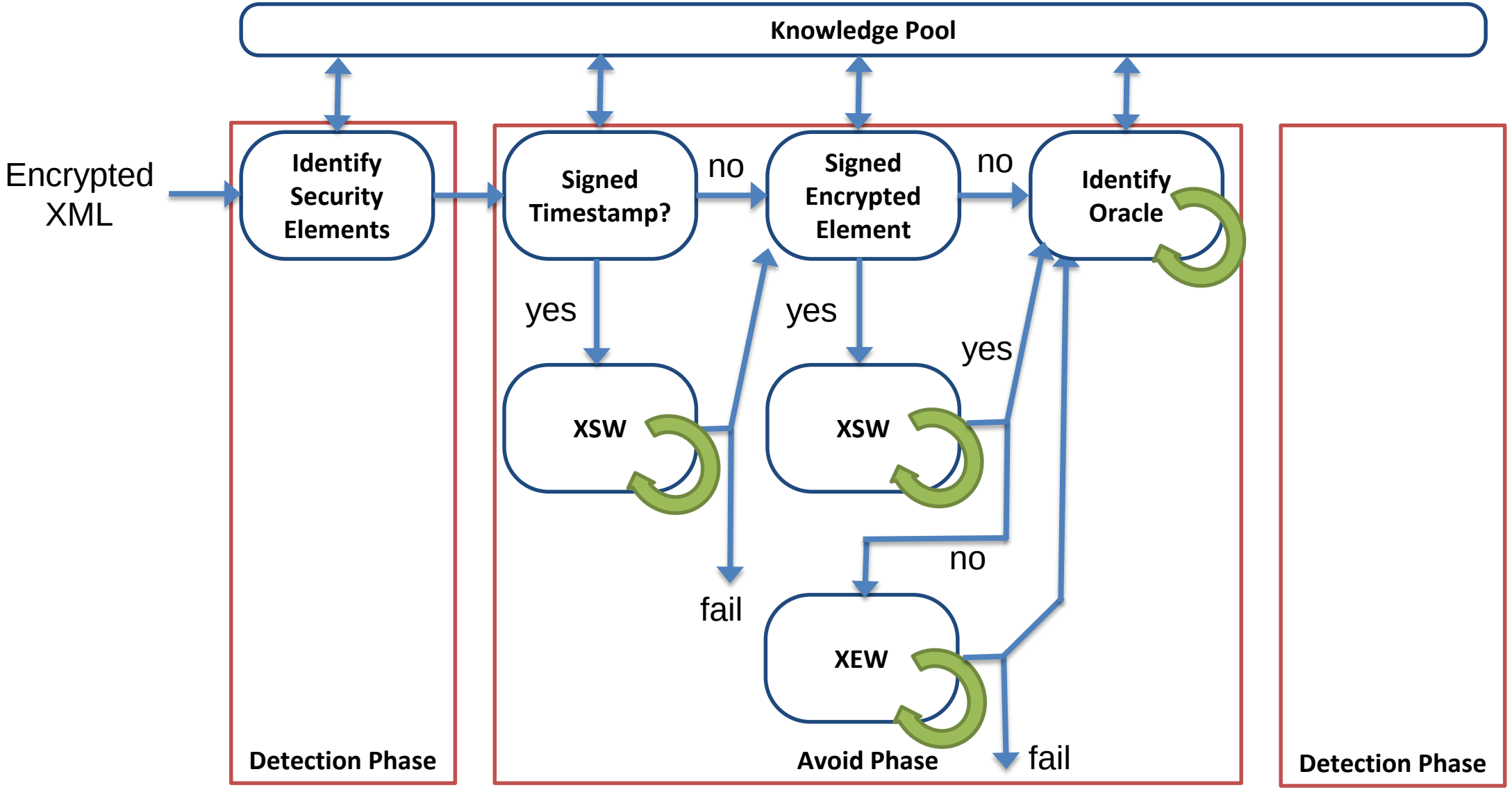
Automated Attack Workflow



Applying XSW - Complexity

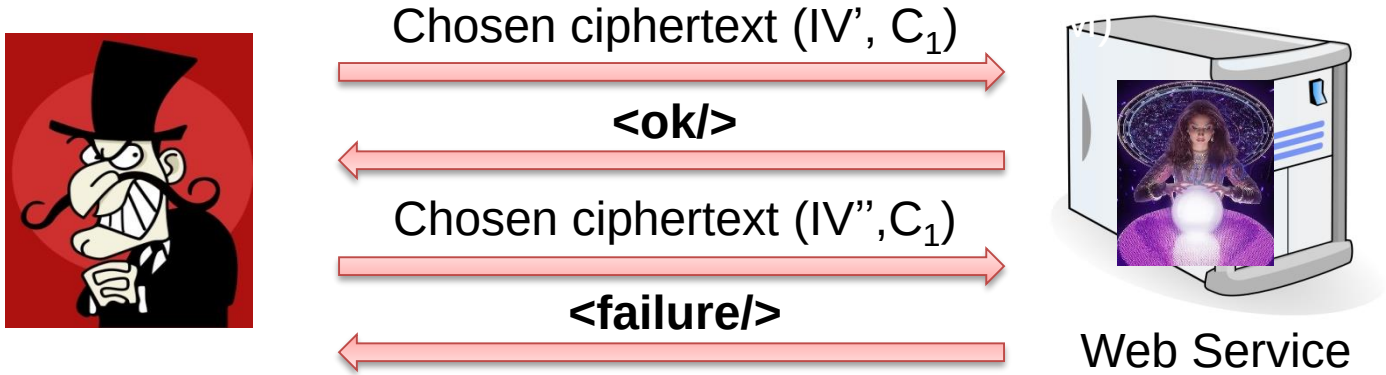


Automated Attack Workflow



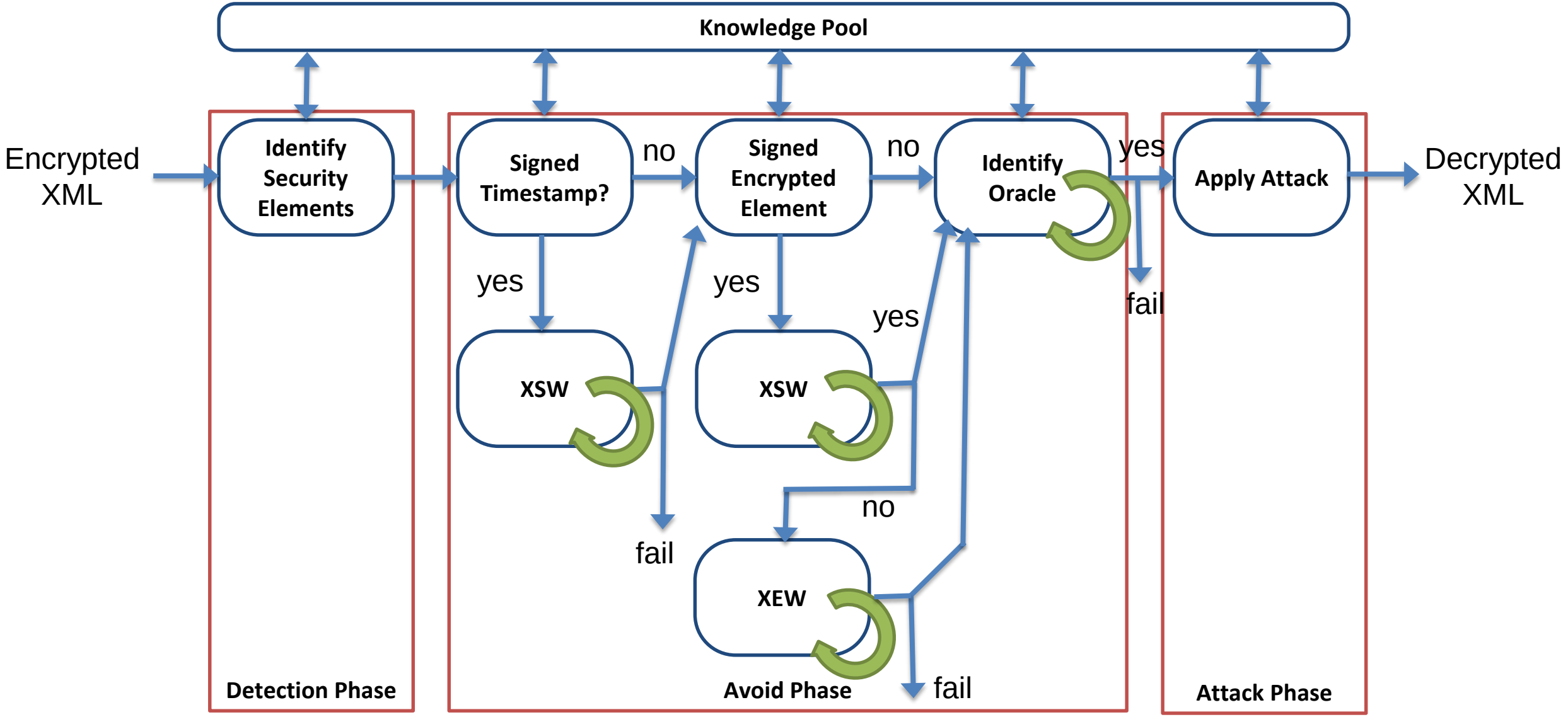
Identify Oracle

- Map Server Responses to „valid“ or „invalid“



- Implementation dependent!

Automated Attack Workflow



Results

System	Asymmetric Attack	Symmetric Attack	Countermeasures applicable?
Apache Axis2 1.6.2		✓	
Apache CXF 2.7.10	✓	✓	yes
Axway Gateway 7.3.1	✓	✓	yes
IBM Datapower XI50		✓	yes
Microsoft WCF			yes









Conclusion

- XML – especially XML Security – is complex
- WS-Attacker can be used to test Web Service implementations automatically
  - https://github.com/RUB-NDS/WS-Attacker
- Our approach is applicable to other scenarios
  - SAML, JSON, …
- Preffer authenticated encryption (AES-GCM instead of AES-CBC)



Q&A?