Plasma Protected IODEF

https://datatracker.ietf.org/doc/draft-schaad-mile-iodef-plasma/

Dr. Trevor Freeman
Senior Security Strategist
Trustworthy Computing
Microsoft Corporation

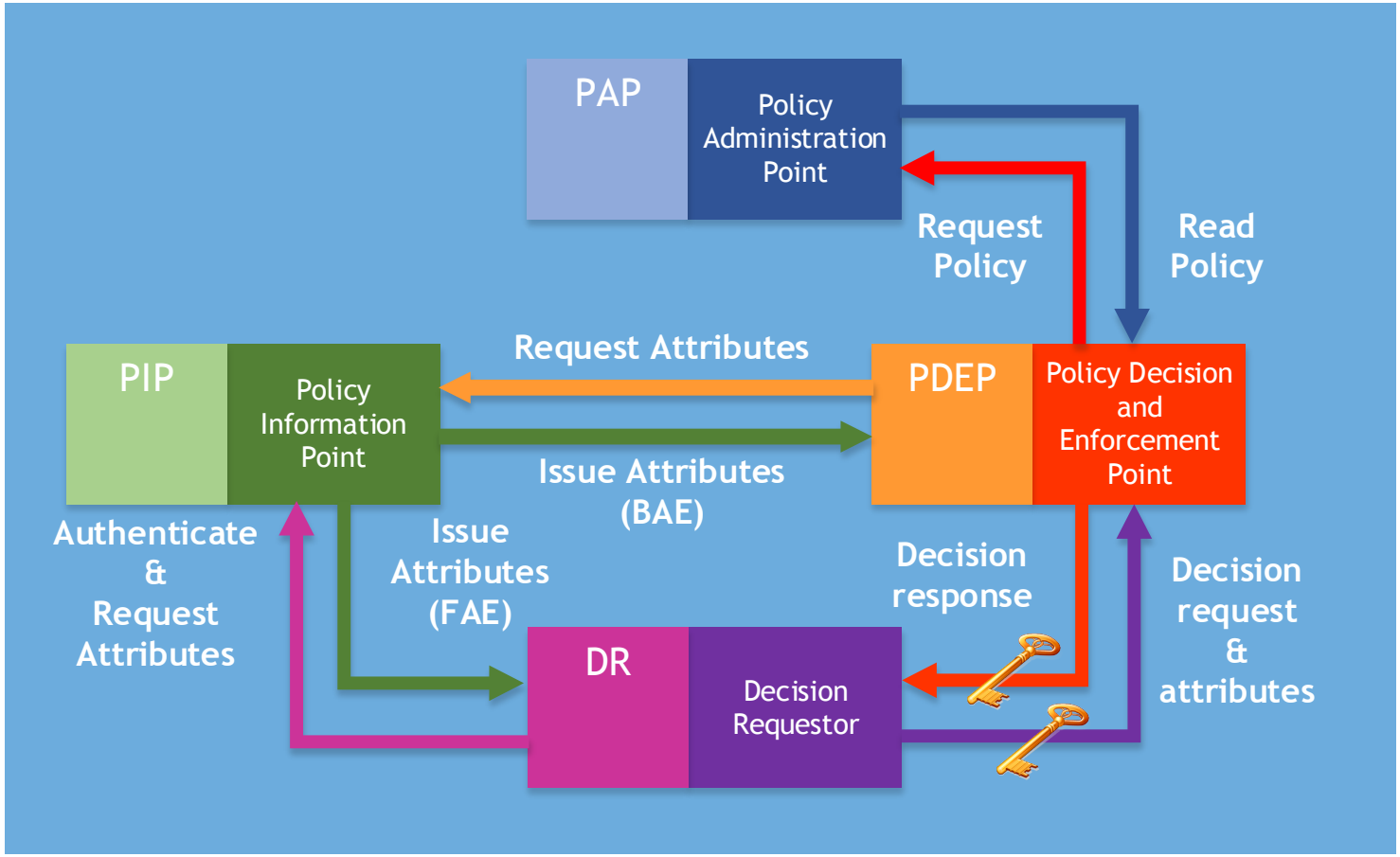
Agenda

- Plasma and Email
- Plasma and IODEF

Plasma & Email

- Update S/MIME in two key areas
  - Provide viable access control mechanism
    - Address limitations of rfc2634 (Enhanced Security Services for S/MIME)
  - Remove dependency on X.509 certificates

Plasma Data Model



Plasma IETF Drafts

Plasma Request Protocol

- General purpose decision request\response
  - DR policy set discovery
  - DR send protected message
  - DR read protected message
- Tokens for authentication and attributes
- Obligations for encryption, signing, visual marking

https://datatracker.ietf.org/doc/draft-schaad-plasma-service/

S/MIME Updates

- Marking policies on S/MIME message
- ASN.1 encoded policy metadata
- Features
  - Access decision prior to access to data
  - Backwards compatible with existing S/MIME

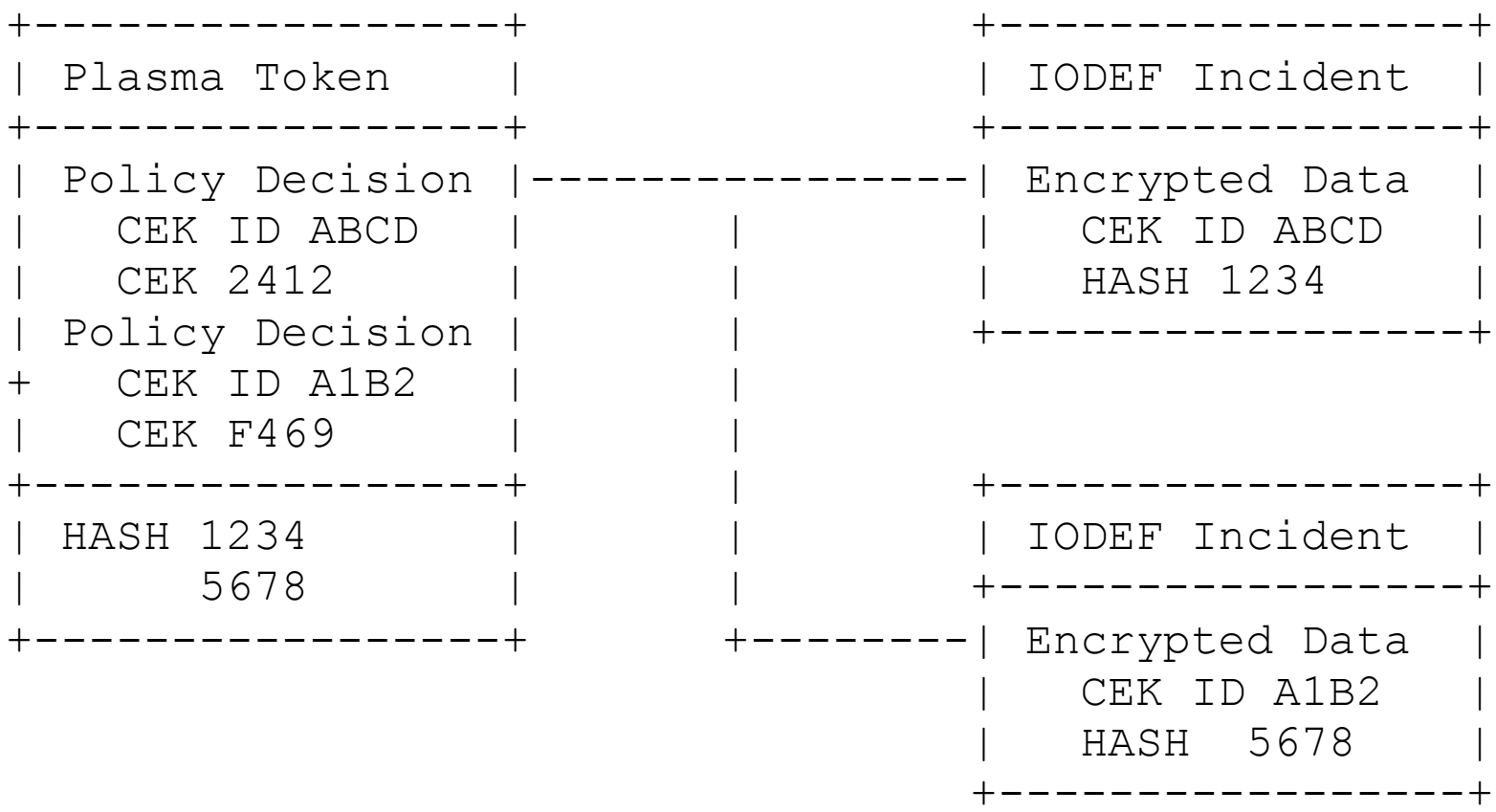
https://datatracker.ietf.org/doc/draft-schaad-plasma-cms/

Plasma & IODEF

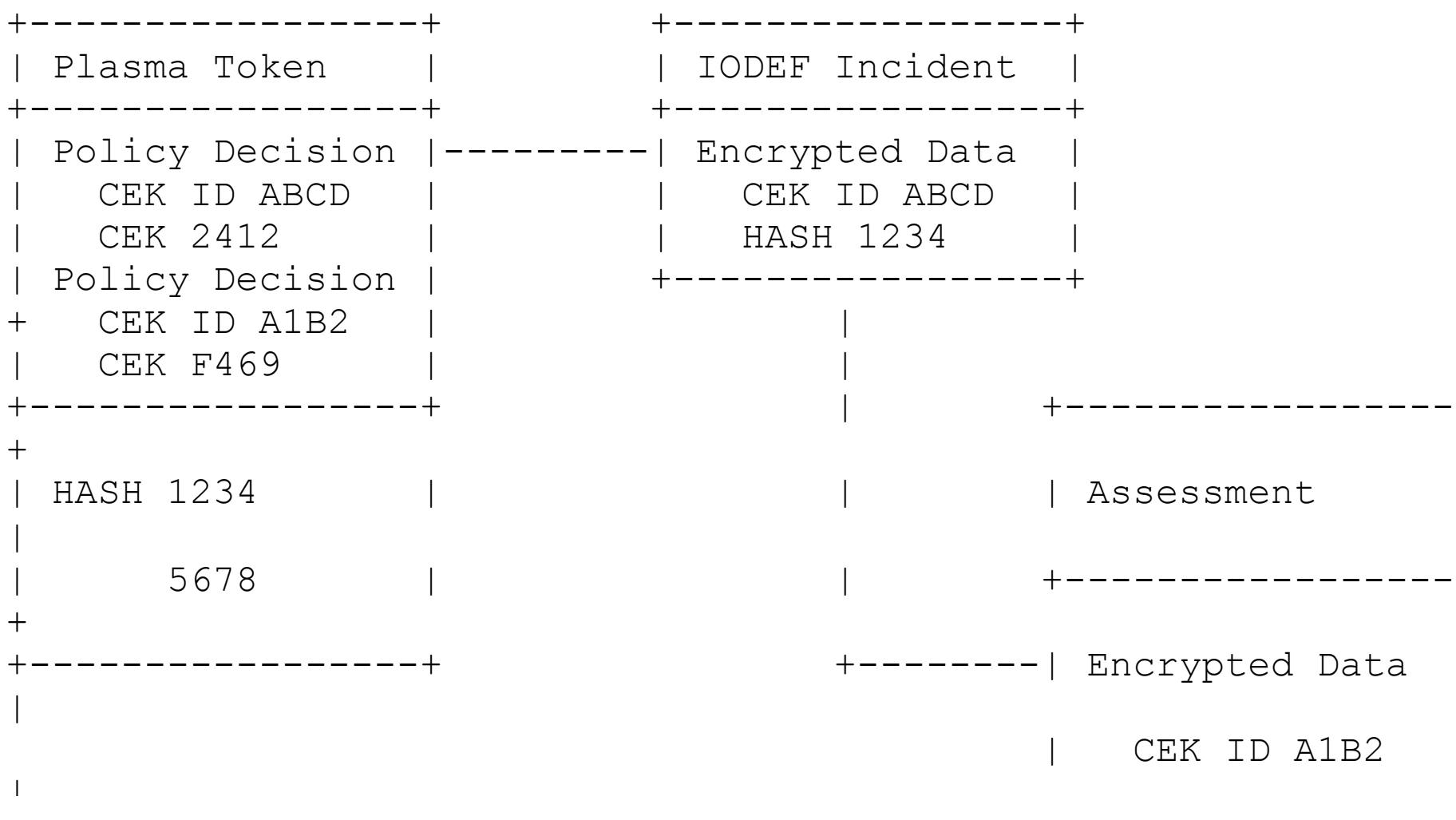
- XML encoded Plasma token
  - Semantically the same as email Plasma token
  - Stored in Additional Data class of IODEF document
  - Protects incidents or incident sub classes
- Uses Plasma Service protocol
- Single token supports multiple access control decisions
- Binding between protected data and token via encryption keys

Single Decision, Multiple Incidents

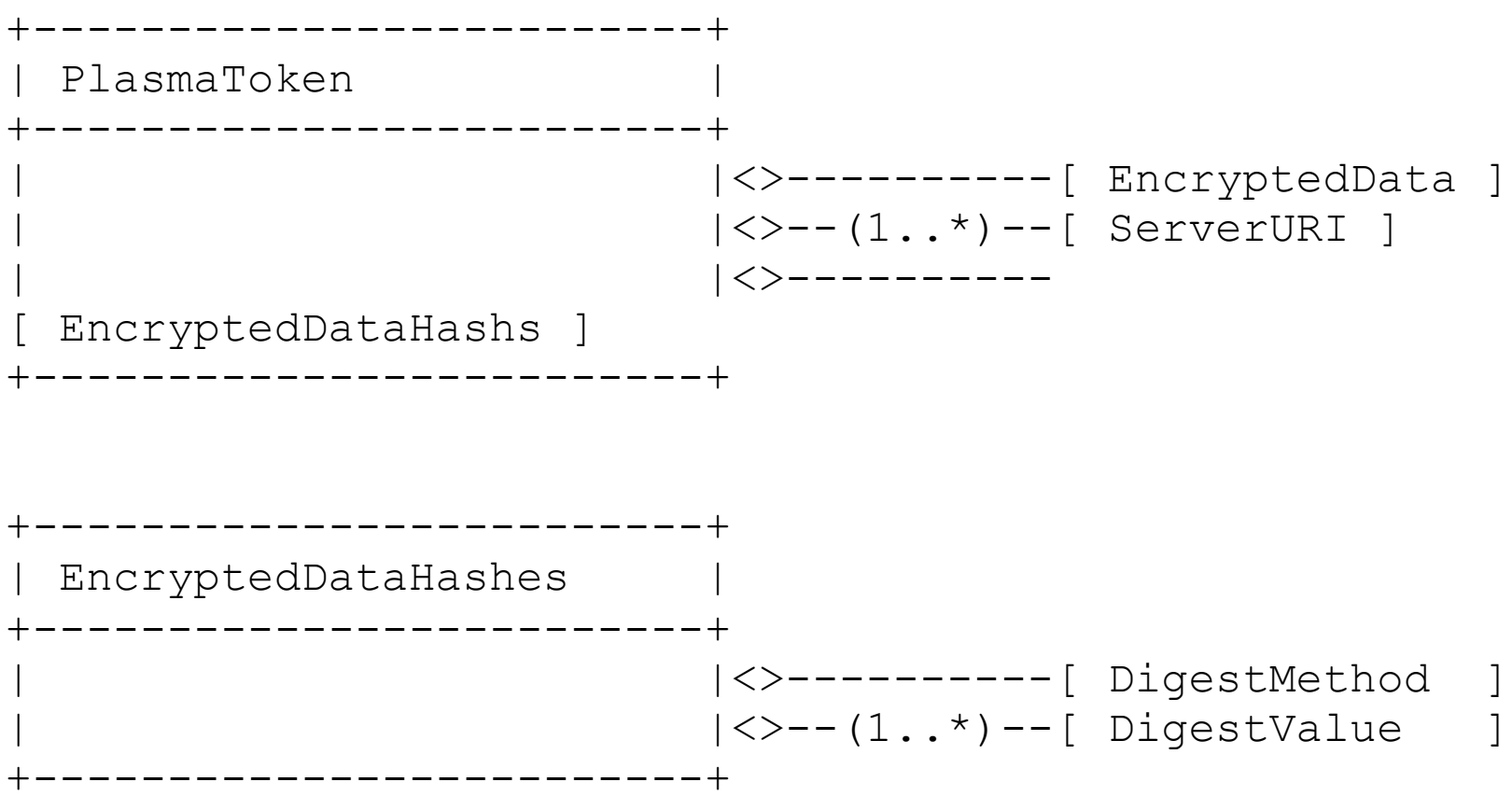
Multiple Decisions, Multiple Incidents



Multiple Decision, Single Incident



Plasma Token Class



IODEF Encrypted Class Schema

```
<xs:element name="IODEF-Document">
       <xs:complexType>
           <xs:sequence>
               <xs:group ref="iodef:IncidentChoice‟ maxOccurs="unbounded"/>
           </xs:sequence>
           <xs:attribute name="version" type="xs:string‟ fixed="1.00"/>
           <xs:attribute name="lang" type="xs:language" use="required"/>
           <xs:attribute name="formatid" type="xs:string"/>
       <xs:complexType>
   </xs:element>

   <xs:group name="IncidentChoice">
       <xs:choice>
           <xs:element> ref="iodef:Incident"/>
           <xs:element name="EncryptedIncedent type="xenc:EncryptedDataType"/>
       </xs:choice>
   </xs:group>
```

Plasma Options for IODEF

- Plasma Lite
  - Unencrypted data with Plasma token
- Capability Based Access Control Filtering

	TLP	Plasma Lite	Plasma
Policy Extensibility	None	Extensible	Extensible
XACML Support	No	Yes	Yes
Tamper Resistance	None	Tamper Evident	Tamper Proof
Transport Security Dependency	Yes	Yes	No
Application Impact	Minimal	Minimal	Moderate
Encryption at rest protection	No	No	Yes
Transport Topology	Any	Point-2-point	Any
PII\Sensitive Data Protection	Minimal	Partial	Full

Questions

Dr. Trevor Freeman
trevorf@microsoft.com
Trustworthy Computing
Microsoft Corporation