

XKMS Overview

Thomas Hardjono

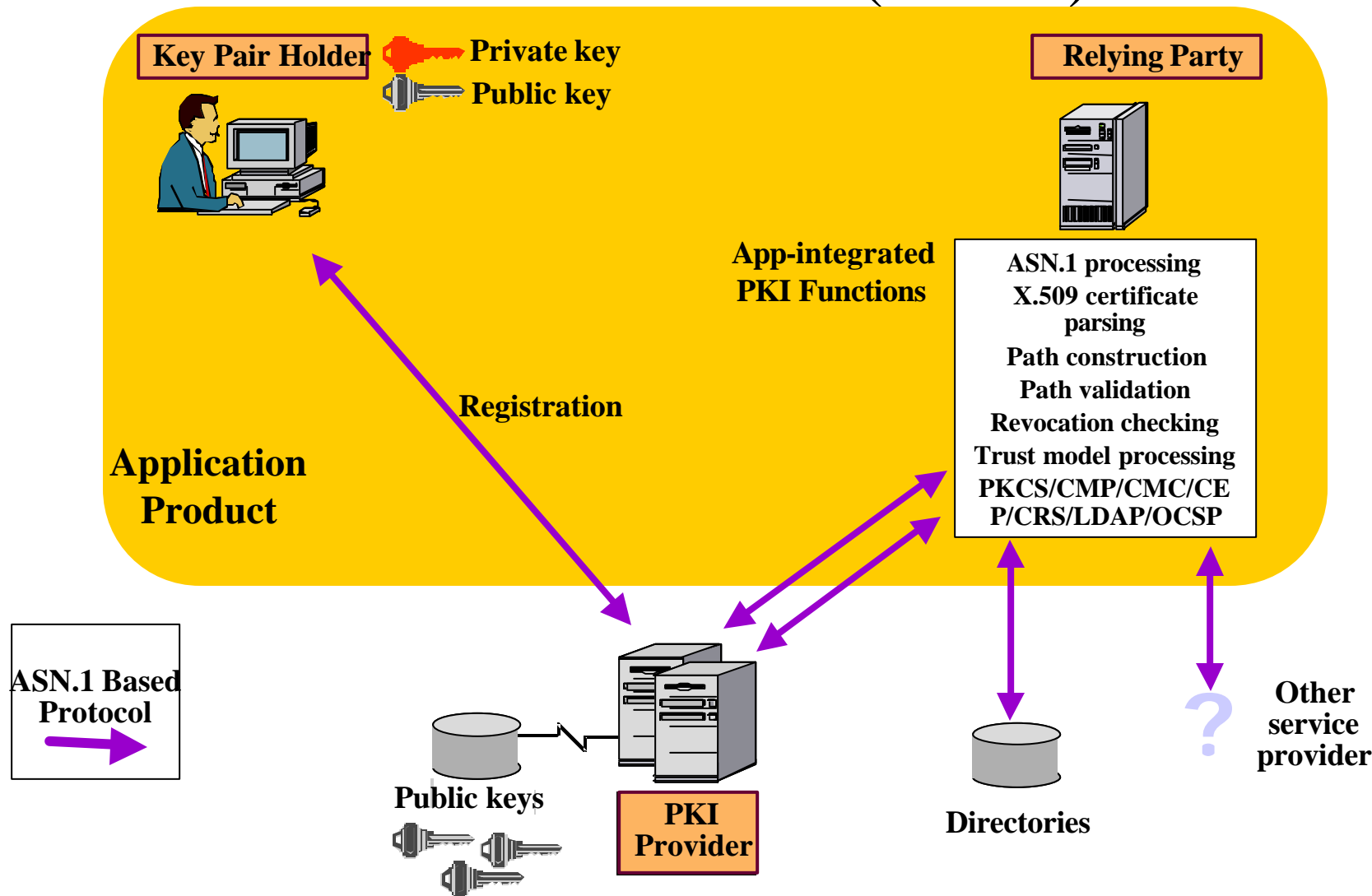
VeriSign

thardjono@verisign.com

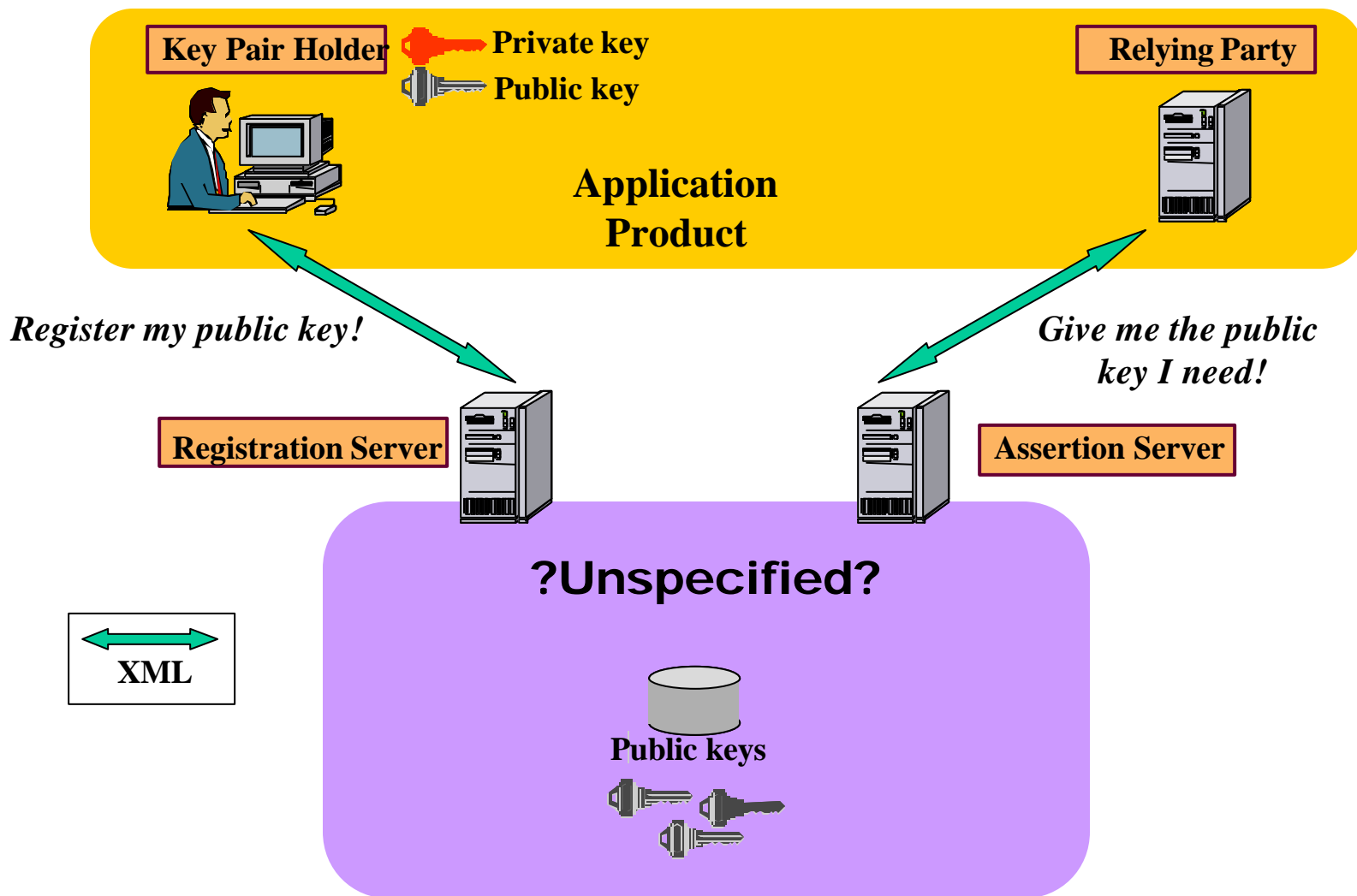
Problems with PKI today

- Burden is on the client to perform costly operations:
 - ASN.1 encoding/decoding
 - Signature verification
 - Chain validation
 - Revocation checking
- Difficult and costly to interface applications to PKI service infrastructures:
 - Proprietary PKI-vendor toolkits typically needed
 - Complex functions need to be embedded in applications
 - Need different solution for different infrastructure vendors
- Need to offload X.509 Processing:
 - XML presents opportunity to incrementally and easily add access to new trust services to applications

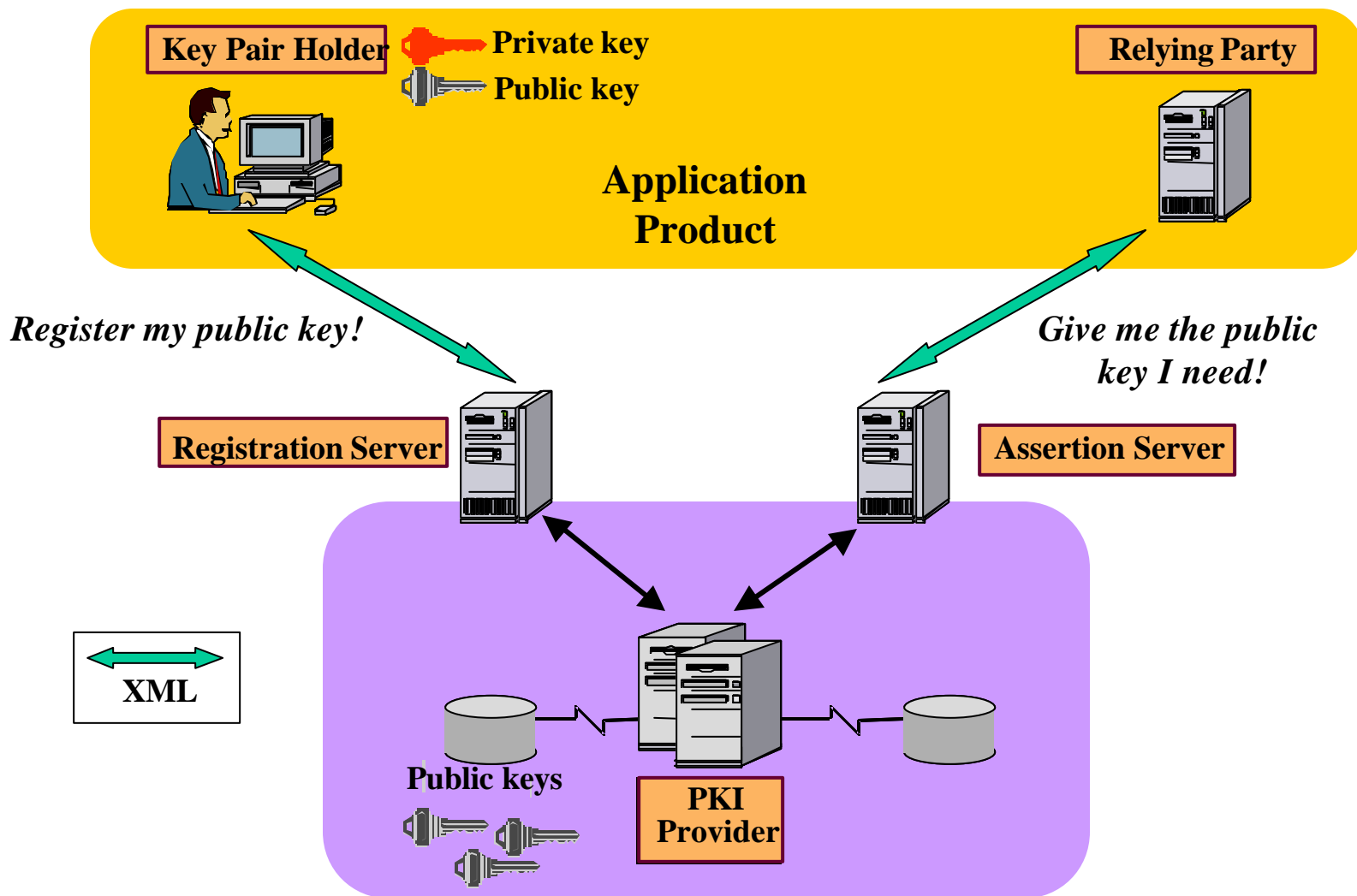
X.509 PKI Model (PKIX)



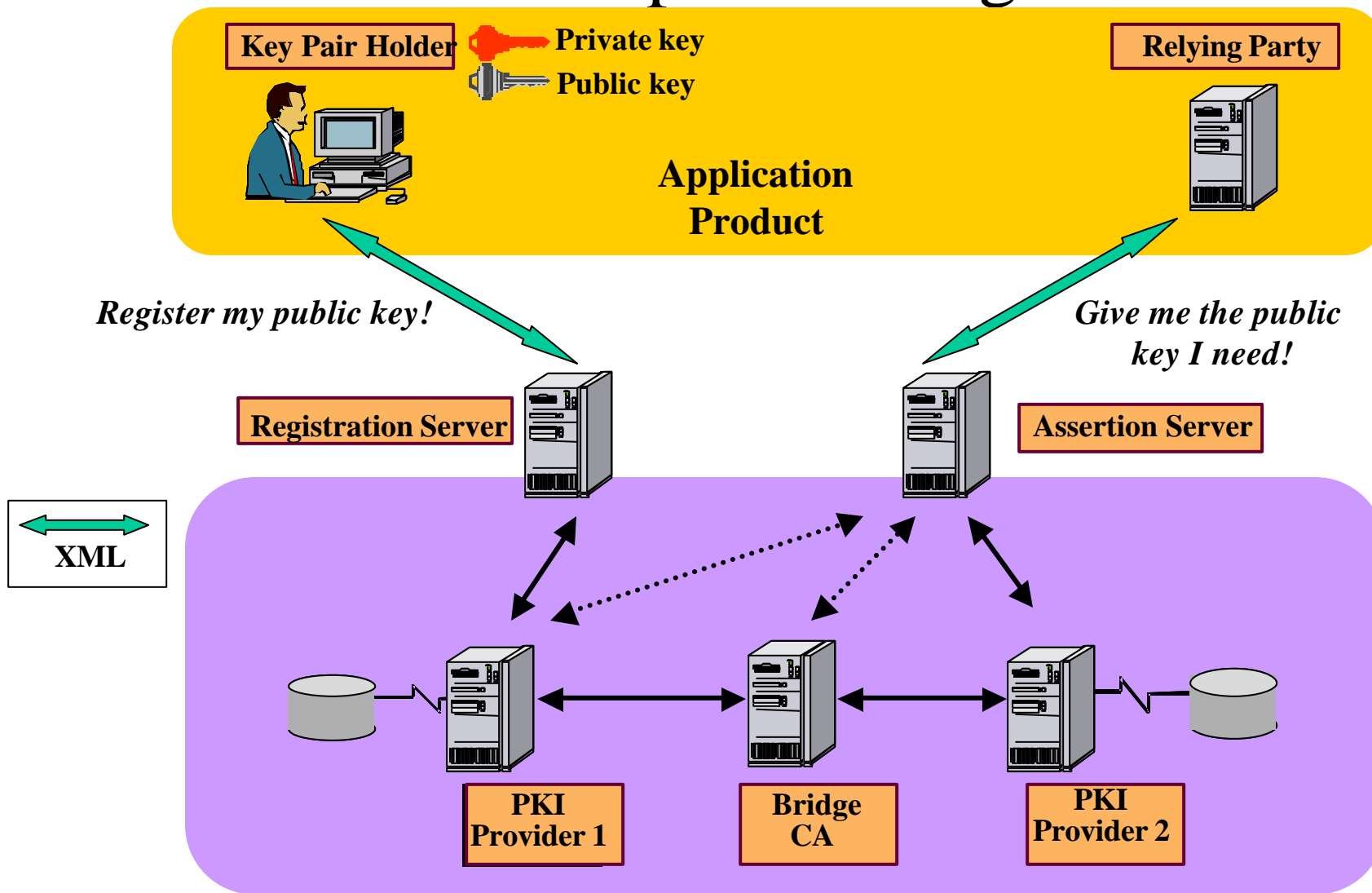
XKMS Model



XKMS: Simple Configuration



XKMS: Complex Configuration



XKMS Characteristics

- Compatible with X.509 PKI
 - But not necessarily bound to that type of underlying PKI
- Can transparently support arbitrarily complex underlying trust/policy structure
 - Examples: Federal Bridge CA; mixture of X.509 and non-X.509
- Leverages with XML Signature & Encryption
- Application product:
 - Must implement basic sign/verify ops and manage a private key
 - Must generate and process limited XML transactions
 - Does not need ASN.1 or X.509 chain processing
- Extensible
 - Example: Authorization/attribute information can be delivered with public key
- Consists of X-KISS, X-KRSS, X-BULK

X-KISS

- *X-KISS: XML Key Information Service Specification*
- Defines protocols to support the processing by a relying party
 - key information associated with a XML digital signature,
 - XML encrypted data,
 - or other public key usage in an XML-aware application
- Current main functions:
 - Certification location
 - Certificate validation

X-KRSS

- *X-KISS: XML Key Registration Service Specification*
- Defines protocols to support the registration of a key pair:
 - Registration.
 - Revocation.
 - Recovery.
- Permits delegation of trust processing decisions to one or more specialized trust processors
- The trust and integrity of XMKS responses received from a XMKS-responder through the use of XML Signature

X-BULK

- *XML Key Management Specification Bulk Operation*
- Used for bulk registration
 - E.g. Device certificates (in Smartcards, cable-modem, TCPA).
 - Reuses element definitions from the X-KRSS specification
- Main differences between X-KRSS and X-BULK include:
 - X-BULK is required to correlate batches of requests & responses.
 - X-KRSS does not support some legacy key registration formats (e.g. PKCS#10) used in many existing hardware modules.
 - Notion of batch-status vs. key-status

XKMS Status

- Original submission of spec by VeriSign, Microsoft and WebMethods
 - March 2001
- Working Group in W3C: *XML Key Management WG*
 - WG established in March 2002
 - See: <http://www.w3.org/2001/XKMS/>
 - Current spec is version – March 2002
- Other links:
 - <http://www.xmltrustcenter.org>

END
+
Thank You