XML Key Management Specification (XKMS)

April 2001

Recent Developments

- XML Signature standard proposal completed
- XML Encryption companion standard in development
- Industry collaborators announce compatible key management specification
  - XML key management specification (XKMS)

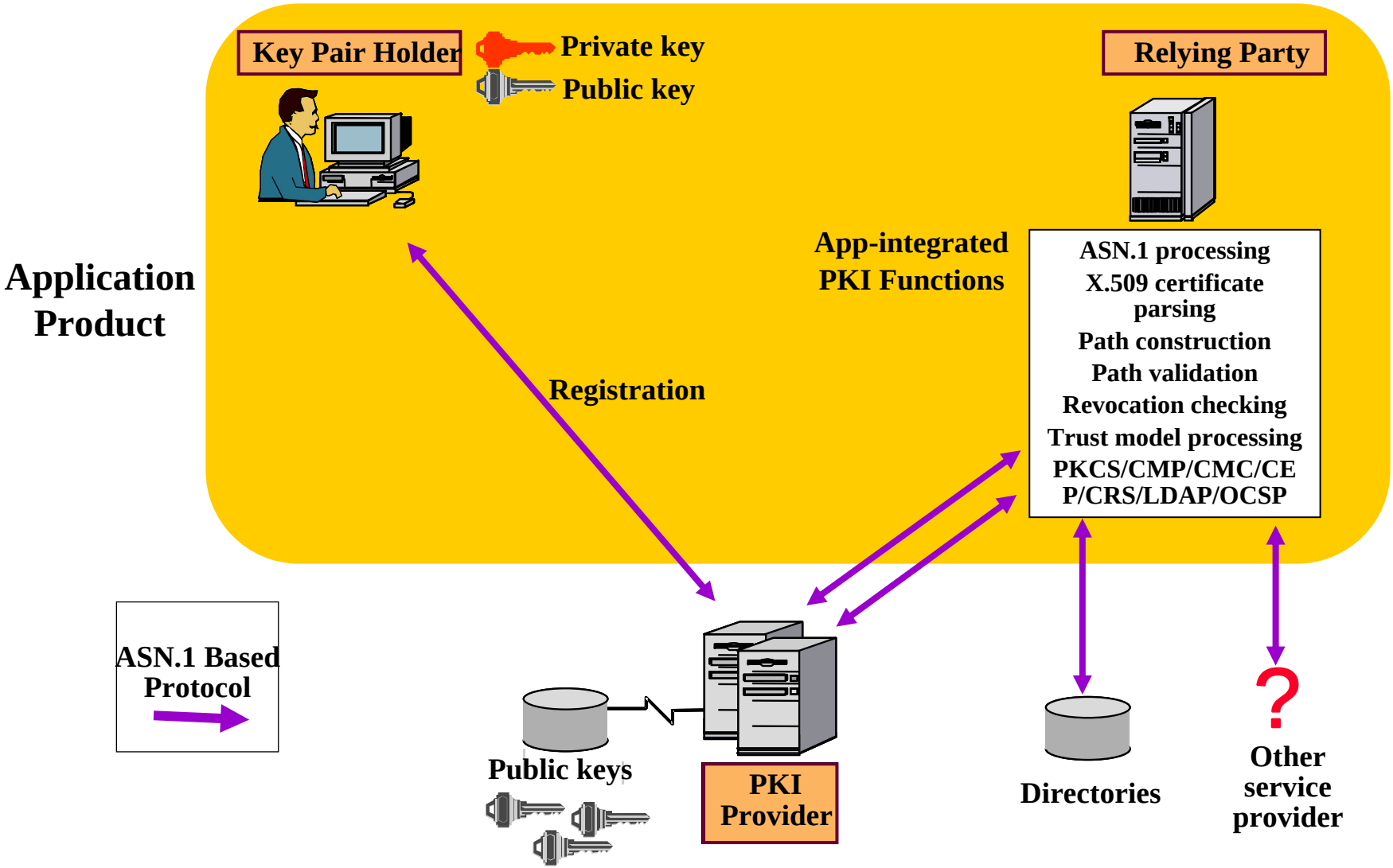
PKI Application Enablement

- It has been 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 infrastructures
- XML presents opportunity to incrementally and easily add PKI services to applications

PKI Second Generation

- Deployed either…
  - Fully embedded (e.g., DOCSIS); or
  - Applications see simple, standard plug-and-socket
- Menu of application-oriented functions
  - Register this public key!
  - Give me the assured public key for this signature!
  - Verify this signature!
  - Is this signer authorized?
  - Notarize this transaction!
- Any complexity hidden *under the hood* in the infrastructure
- Transparent to the user

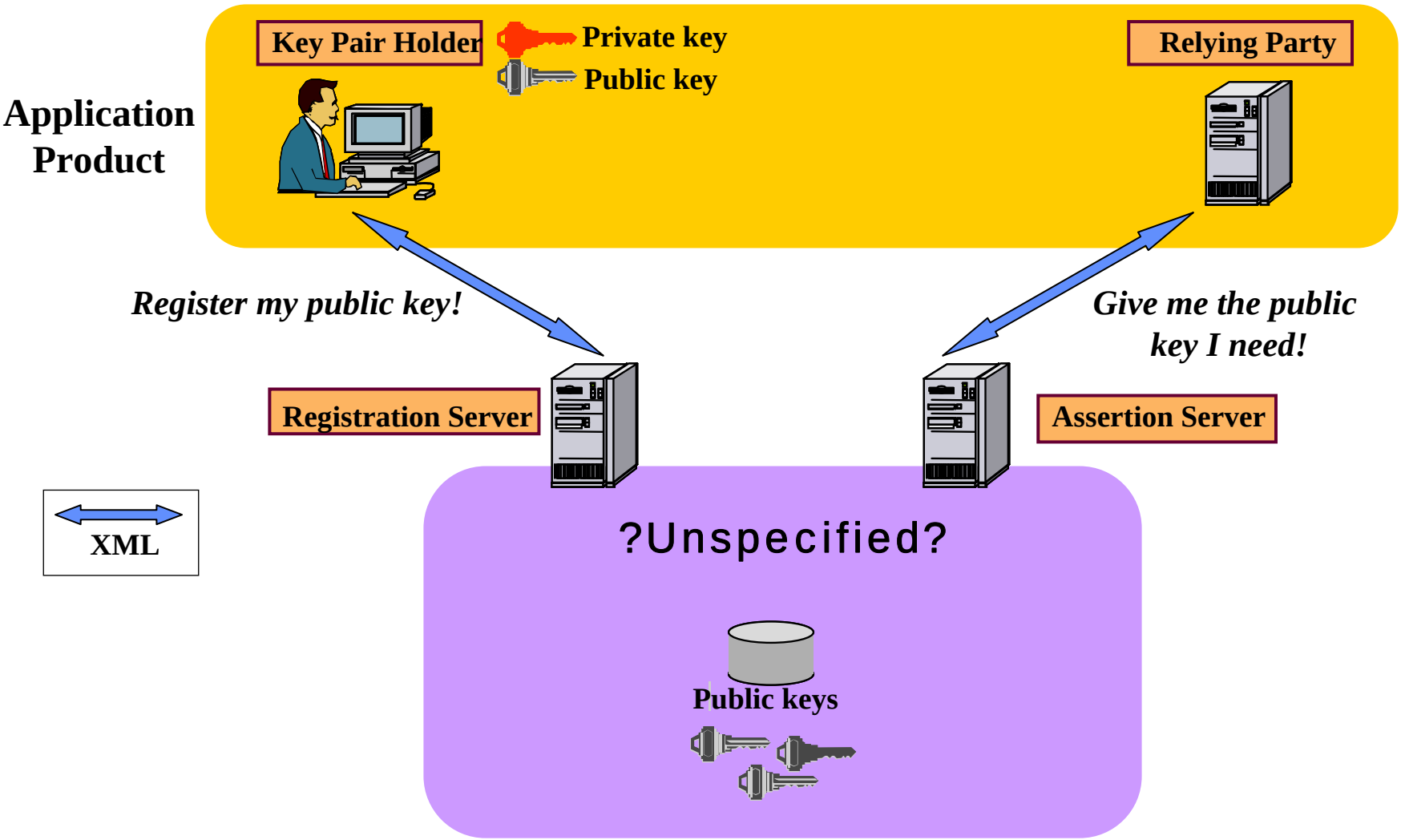
X.509/PKIX PKI Model



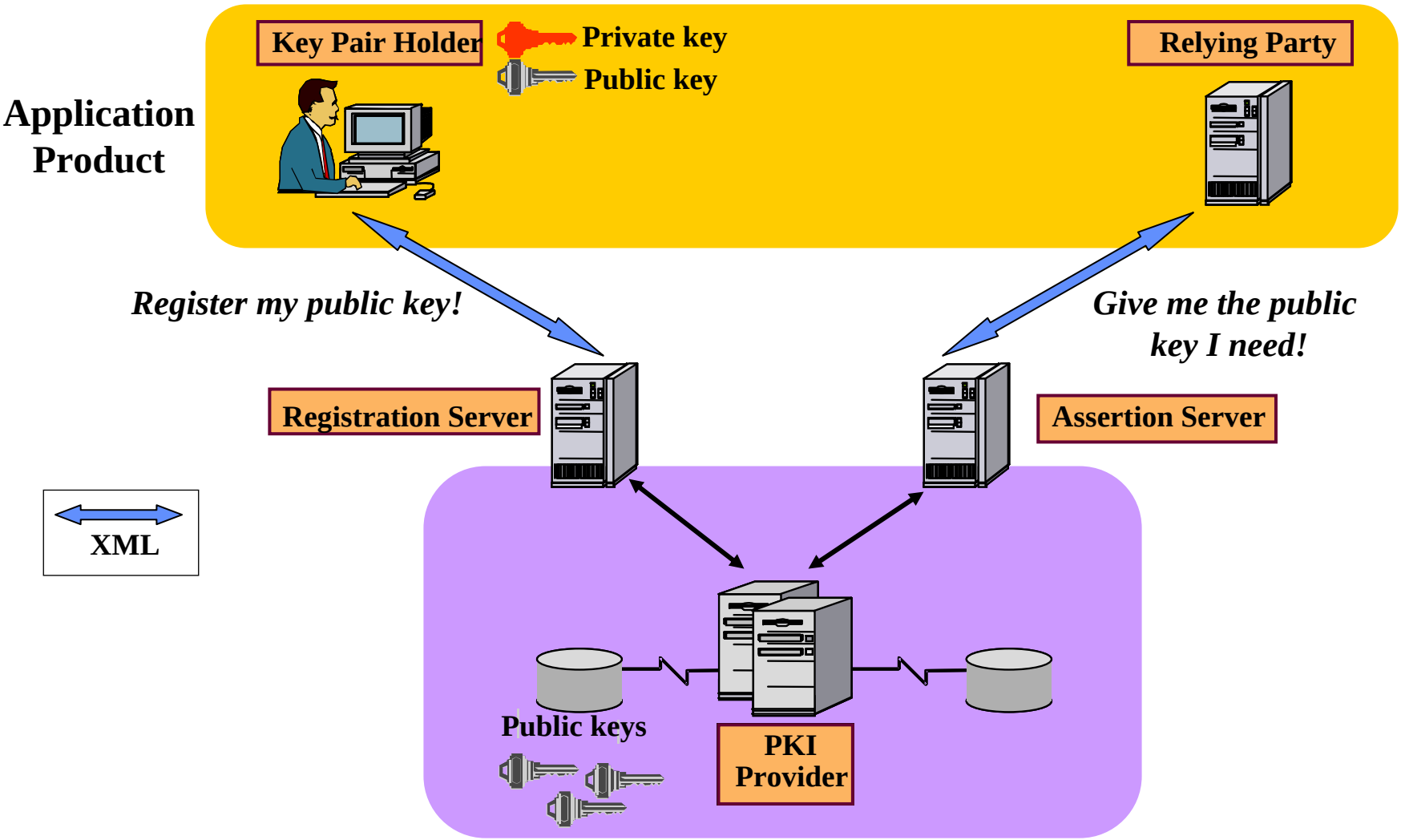
Offloading X.509-Processing

- OCSP
  - Offloads revocation status checking to a server
- OCSP-X or SCVP
  - Offload (or delegate) X.509:
    - Certificate path discovery (DPD); and/or
    - Certificate path validation (DPV)
  - Simplifies the processing functions that app needs to incorporate, but app still needs to understand X.509 certificates, paths, and ASN.1

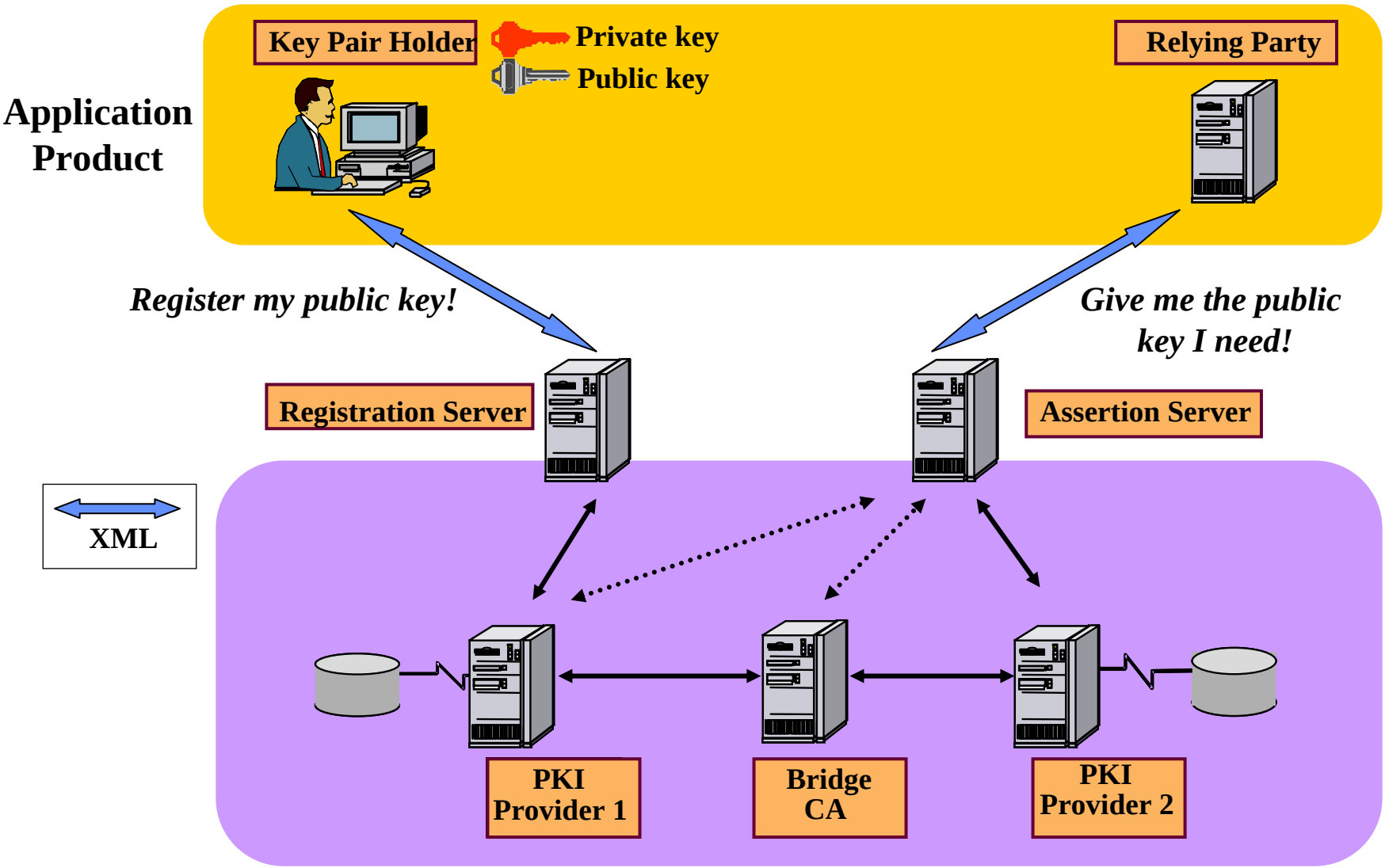
XKMS Model


Application Product
Key Pair Holder
Private key
Public key
Relying Party
Register my public key!
Give me the public key I need!
Registration Server
Assertion Server
XML
?Unspecified?
Public keys

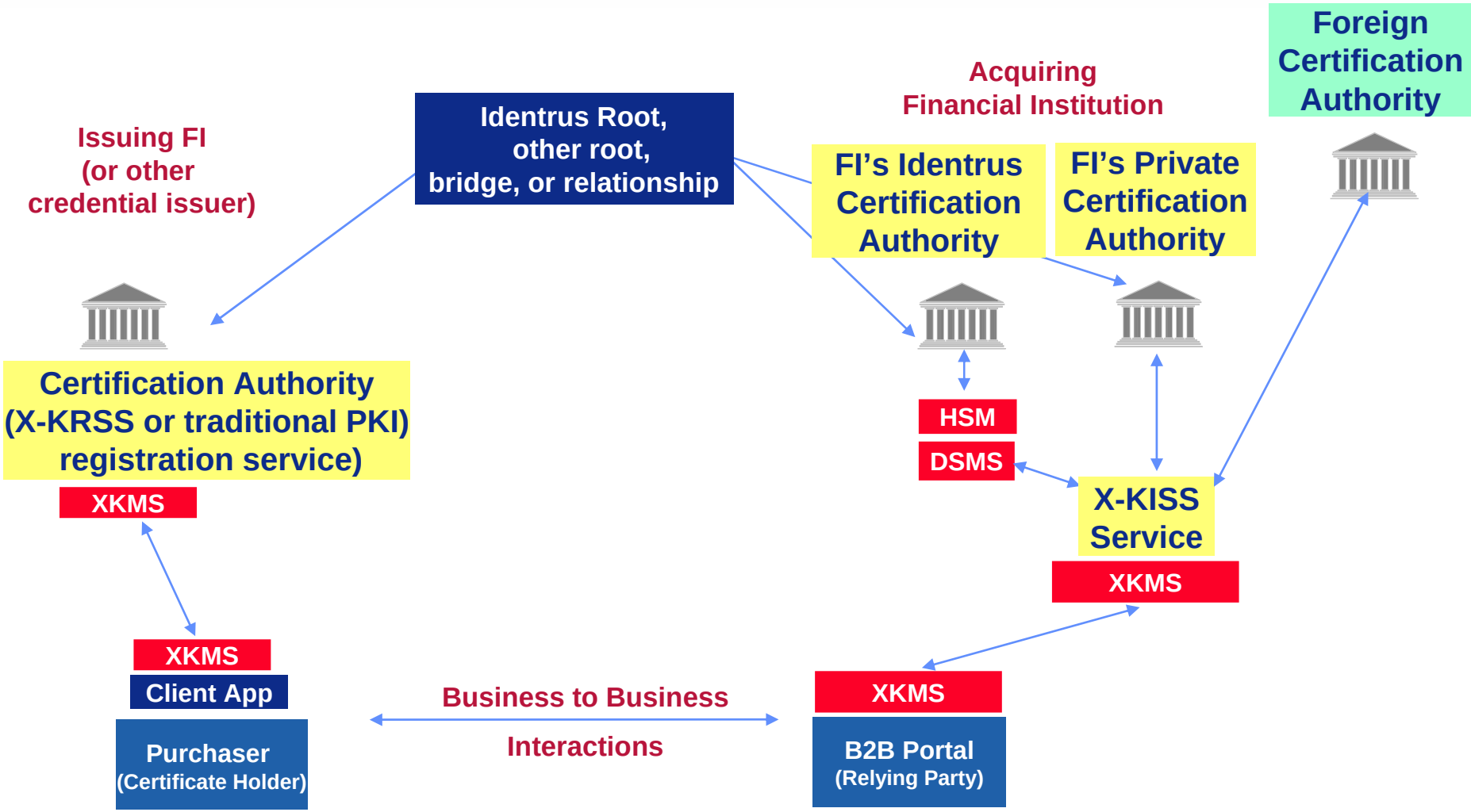
XKMS - Simple Configuration



VeriSign™ XKMS - Complex Configuration



VeriSign™ Multi-PKI Backend Using XKMS



XKMS Status Summary

- Developed by VeriSign, Microsoft, webMethods
- Supported by IBM, HP, iPlanet, Baltimore, Entrust, RSA, IONA, PureEdge, Evincible, Citigroup, Reuters, SAIC, CIBC
- Submitted to W3C with proposal to formally standardize

Interoperability Programs

- Developer site: www.xmltrustcenter.org
- VeriSign SDK available for download
- Trial service available for developers
- Several vendors participating in informal interoperability testing
- Evincible XKMS application demonstrated at RSA 2001

Summary - 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, e.g.: Federal Bridge CA
- Compatible with XML Signature & Encryption, XML Protocol
- Application product:
  - Must implement sign/verify ops and manage private key
  - Must generate and process limited XML transactions
  - No ASN.1 or X.509 chain processing
- Extensible
  - Example: Attribute information delivered with public key
  - Can work in conjunction with services like SAML
- Broad industry support - open standard